



サプライチェーン リスクマネジメント実態調査

—リスク管理投資は1億円未満が約半数
—**全社横断体制・投資・人材面に残る課題**—



目次

01	はじめに	3
02	エグゼクティブサマリー	4
03	調査結果から見えたサプライチェーンリスク管理の現在地	5
	・ 偏る懸念と進まぬ対策 ——リスク認識と対応状況に見られるばらつき	5
	・ リスク評価 「売上」「事業継続」を重視 非財務視点の組み込みに余地	7
	・ 部門主導、限定的な投資、人材不足——経営アジェンダと隔たり	8
	・ デジタル活用は進むも 見えぬ供給網に半数が不満	11
	・ 高まる規制・技術の壁——外部専門家起用も 活用範囲は限定的	13
04	強靱なサプライチェーン構築に向けた5つの変革	15
05	供給網を蝕む4つの脅威——領域ごとの実態と企業が取るべき対策	18
	・ 災害	18
	・ 品質	23
	・ サイバーセキュリティ	29
	・ ESG／環境／人権／労務	33
	参考データ	39

はじめに

変わるサプライチェーンの前提 多様化するリスクへの備えはあるか

自然災害、サイバー攻撃、地政学的緊張、経済安全保障——。企業を取り巻くリスクが、多様化・複雑化しています。1つ1つのリスクが経営に与えるインパクトは大きいだけに、問題発生時に「不測の事態」として片づけることは、これまで以上に難しくなりました。

特に警戒すべき領域の1つが、地域・国境・企業間をまたぐサプライチェーンでしょう。長大な鎖のどの部分に、いつ、どういったリスクが絡むか分からず、生じる問題によって企業が受ける被害は多岐にわたります。自社が財務的な損失を被るだけで済むとは限りません。社会的な問題につながることでブランド価値は大きく毀損し、企業活動が麻痺すれば顧客や取引先の事業にも影響を与えるでしょう。

意識しなければならないのは、サプライチェーンが、もはや単なる調達や物流の機能ではないということです。複合的なリスクに常にさらされている企業活動の生命線だと認識を改め、事業継続の前提に織り込まなければいけません。いち早く危機意識を引き上げ、レジリエンス(強靱性)を高めた企業は、この先も他社に比べて競争優位を確保しやすくなるという裏返しでもあります。

こうした問題意識に立って、PwC Japanグループはサプライチェーンリスク管理の実態と課題を捉えるために国内調査を行いました。多様な業種・規模の企業の部門長から経営幹部までを対象に、サプライチェーンを取り巻く12のリスクへの意識や対応状況などを集計。数々のリスクについて、どの程度「経営課題」として捉え、どこまで対策に踏み込んでいるのかを検証しました。本調査で確認されたのは、多様なリスクを認識しつつも、具体的な対策や十分な投資につながない状況です。

本稿では調査から見た日本企業の現在地を明らかにした上で、取り組むべき5つの施策をまとめました。加えて、特に対応が求められる主要な領域について、調査結果を踏まえつつ、実務上の課題と対策を整理しています。これらのデータや知見が、日本企業のサプライチェーンリスク管理強靱化の一助となれば幸いです。

【調査概要】

調査目的	日本企業におけるサプライチェーンリスクマネジメントの実態把握
調査対象	全国の企業の経営層、経営企画、サプライチェーン・購買・物流、リスク管理、情報システムなどの部門に所属する役職者
有効回答数	288名
調査方法	インターネット調査
調査期間	2025年9月3日～9月11日、10月28日～11月6日

エグゼクティブサマリー

偏る懸念と進め対策

——リスク認識と対応状況に見られるばらつき

サプライチェーンを取り巻く12のリスクへの懸念は、1位が「災害」(60%)で、「サイバー」(47%)「情報漏洩」(40%)が続きました。残る9種類のリスク(「ESG/環境」や「地政学」など)は、6種類が31~38%で3種類が20%台前半にとどまります。一方、対策が「実行・モニタリング段階」にまで達するのは、「災害」でさえ半数をわずかに下回りました。30%台も少なくなく、懸念する割合の低さと同様に、対策の遅れが目立ちます。

リスク評価 「売上」「事業継続」を重視 非財務視点の組み込みに余地

企業がリスクの高さを評価する要素は、いずれも影響額が比較的見積もりやすい「売上」(60%)と「事業継続」(53%)が目立ちます。他方、具体的な企業価値の毀損がイメージしにくい「レピュテーション」は29%にとどまりました。浮かび上がるのは、影響額を見積もりやすい要素に重きを置いてリスクを評価している傾向です。こうした評価軸の偏りによって、レピュテーションの毀損といった非財務領域へのダメージを適正に評価することが難しくなり、「ESG/環境」や「人権/労務」などのリスクに対する懸念の低さや対策の遅れにつながっている可能性があります。

部門主導、限定的な投資、人材不足——経営アジェンダと隔たり

リスク管理については、「各関係部門の会議体」での定期的な検討が44%で、「経営層が出席する会議体」(35%)を上回りました。対応が必要な項目としては「人的リソース・体制の増強」が最多だった他、半数の企業でリスク管理への投資が1億円未満にとどまります。部門主導、限定的な投資、人材不足の背後に透けて見えるのは、少なからぬ企業でリスク管理を経営アジェンダとして十分に認識していないという可能性です。実際、「経営陣・役員のコミットメント」を求める声もあがっていました。

デジタル活用は進むも 見えぬ供給網に半数が不満

デジタルツールの活用では、「環境・人権リスクの評価」(57%)、「サプライヤーの特定」(47%)などの用途が目立ちました。一方で、ほぼ半数の企業が「サプライチェーンリスク管理の全てに対応できていない」という不満を抱えています。ツールの導入は進みつつも、供給網の全体像やリスクを可視化しきれない実態が浮かび上がりました。

高まる規制・技術の壁——外部専門家起用も 活用範囲は限定的

規制や技術の高度化に伴い、サプライチェーンリスク管理において専門性を求められる場面が増えていきます。調査では約7割の企業が何らかの形で外部専門家を起用していると回答しました。ただ、「リスクの洗い出し、優先順位付け」といった調査・分析フェーズが中心で、実行面での活用は限定的です。

調査結果から見えた サプライチェーンリスク管理の現在地

偏る懸念と進まぬ対策——リスク認識と対応状況に見られるばらつき

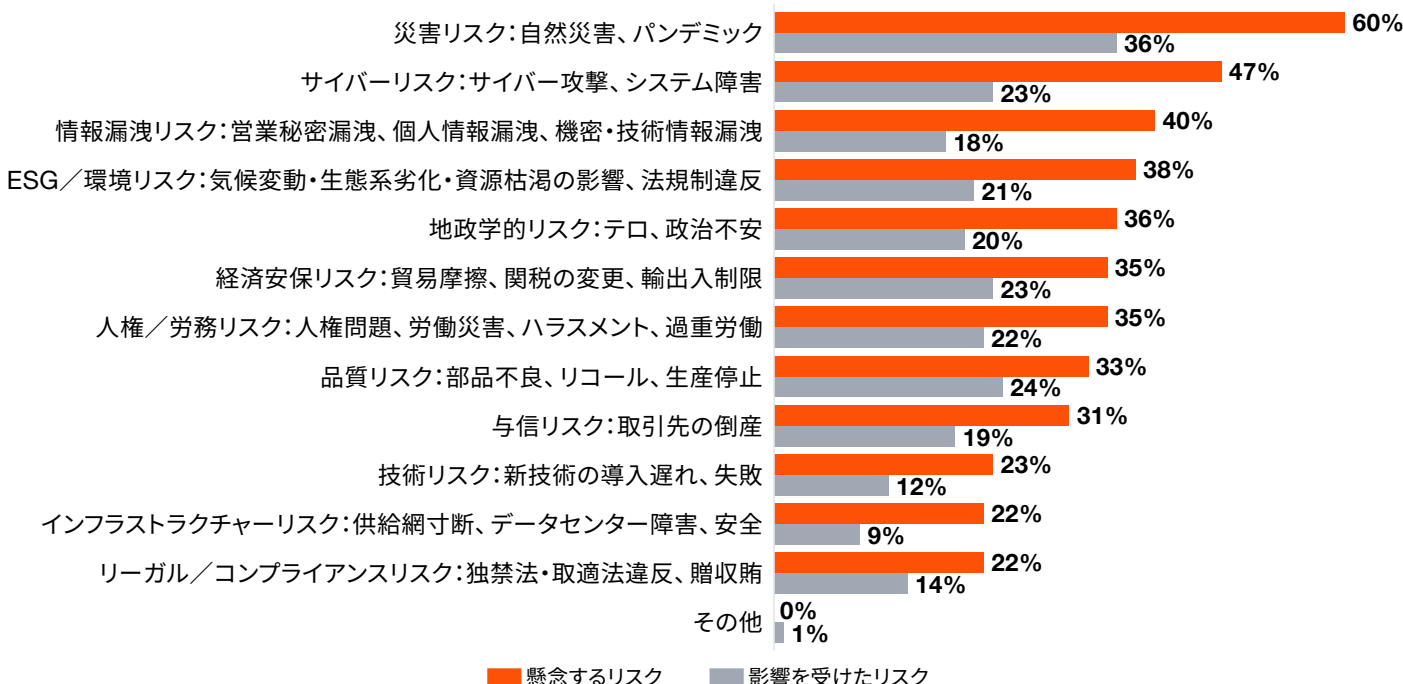
サプライチェーンに絡むリスクが多様化する中、企業の懸念が特に集中したのは「災害」(60%)です(図表1)。頻発する地震や台風などに加え、コロナ禍の経験から、物理的な供給網の寸断を最重要リスクと捉えていることが分かります。続く「サイバー」(47%)や「情報漏洩」(40%)を含め、被害の大きさや実感の得やすさ、そして対応の不備が事業上・社会上の問題に直結しやすいことなどが、懸念の強さに結び付いていると考えられます。

近年注目が集まり始めた「ESG／環境」「地政学」「経済安保」「人権／労務」を含む6つのリスクへの懸念は、31～38%となりました。災害やサイバーに比べると、政治・社会・規制に関連するリスクへの懸念は相対的に低い傾向が見られます。

では、実際に影響を受けたリスクはどうでしょうか。ここでも「災害」が36%と最も高くなったものの、「品質」「サイバー」「経済安保」など6つのリスクも20%台と一定割合の企業が影響を受けたと回答しています。多様化するサプライチェーンリスクが、事業に影響を及ぼす脅威として顕在化し始めていることが分かります。

図表1：懸念するリスクと影響を受けたリスク

Q. 貴社が懸念するサプライチェーン上のリスクおよび実際に影響を受けている／過去に影響を受けたリスクは何ですか。

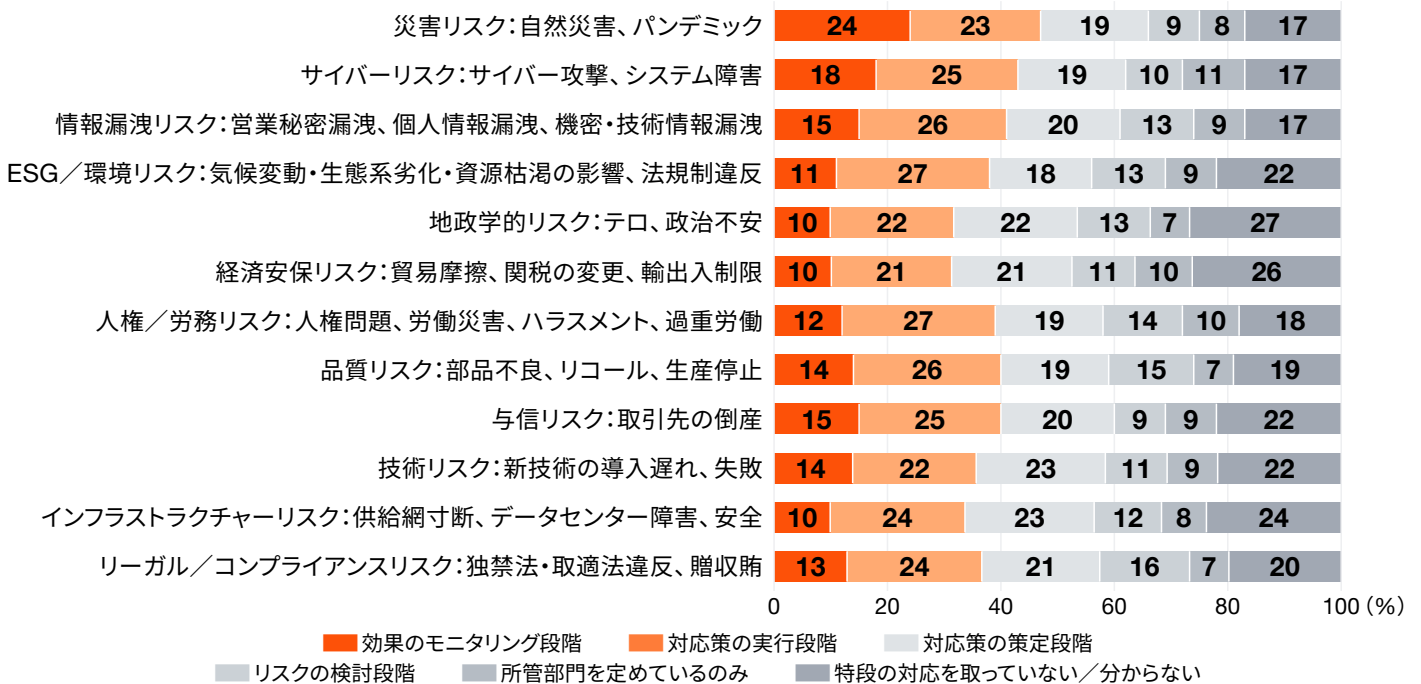


さまざまなリスクが事業に影響を及ぼしつつある一方、対策は進んでいません。対応のフェーズを「検討(所管部門を定めているのみ、リスクの検討段階、対応策の策定段階)」と「実行(対応策の実行段階、効果のモニタリング段階)」に大別すると、最も懸念の高い「災害」ですら、実行フェーズにある企業は半数以下の47%。その他のリスクでも、多くが30%台にとどまりました(図表2)。

これらの結果から、2つの実態が浮かび上がってきます。1つは、「災害」を筆頭に実例が多く、自前で一定程度の対応ができるリスクに懸念や対策が偏りがちなこと。その一方で、ある程度の懸念や実害を認識しているものの、自前ではコントロールしづらい「地政学」や「経済安保」といったリスクに対しては手を打ちかねているということです。こうしたまだら模様のリスク管理体制からの脱却が、喫緊の課題と言えるでしょう。

図表2：リスクへの対応状況

Q. 貴社におけるサプライチェーンリスクへの対応状況について、それぞれ最も近いものをお選びください。



※四捨五入をしているため合計しても必ずしも100とはならない

出所：PwC作成

リスク評価 「売上」「事業継続」を重視 非財務視点の組み込みに余地

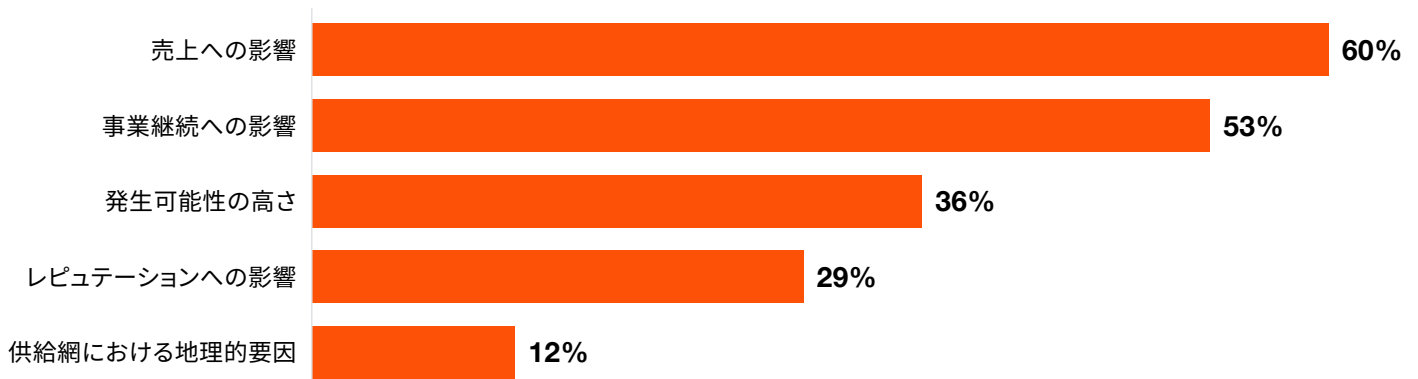
リスクごとの対応状況が大きく異なる背景には、「リスク評価軸の偏り」という構造的な課題が見え隠れします。図表3を見ると、リスクの高さを判断する要素として、「売上への影響」(60%)、「事業継続への影響」(53%)が目立ちました。影響額が比較の見積もりやすいことから、多くの企業がこれらを重視していることがうかがえます。他方、具体的な企業価値の毀損がイメージしにくい「レピュテーションへの影響」は29%にとどまりました。

売上や事業継続への影響額を軸としたリスク評価は、対策の投資対効果が算出しやすい「災害」などのリスク対応には有効です。ただ、発生確率や被害額の算定が難しい「サイバー」「地政学」「経済安保」などの他、ブランド価値毀損といった非財務面への影響が大きい「ESG／環境」「人権／労務」などのリスクに対しては、懸念の高まりや対策の動きを鈍らせる恐れがあります。図表1や2からも、そうした傾向が見て取れました。ブランド価値の毀損などのインパクトは数値換算が難しいものの、回復には長い時間とコストがかかります。決して軽視できるものではありません。

また、リスクのインパクトを多面的にとらえきれていない場合、優先順位に偏りが生じる可能性があります。影響額の見積もりなどの財務的な視点にとどまらず、非財務的な視点も含めた多角的なリスク評価軸を早期に組み立て、全てのリスクを俯瞰した上で自社が対応すべきものを洗い出していく必要があるでしょう。サプライチェーンリスク管理を、災害対応の延長線上で捉える状況から抜け出せるかが肝になります。

図表3：リスクの判断要素

Q. 貴社のサプライチェーン全体のリスク管理において、リスクが高いと判断する要素は何ですか。



出所：PwC作成

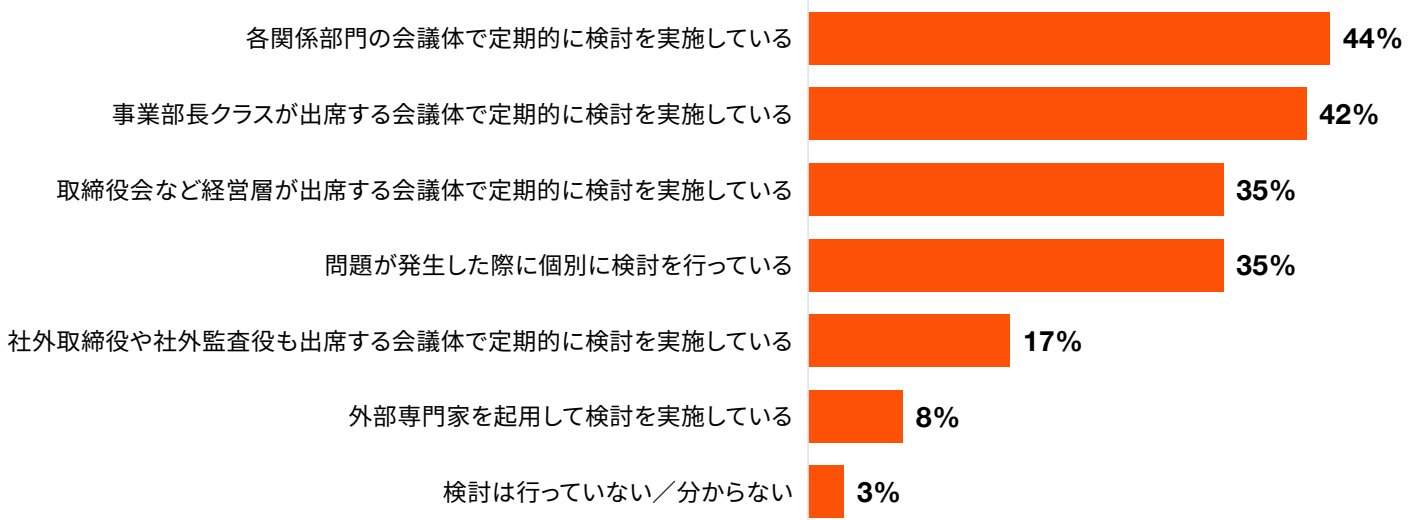
部門主導、限定的な投資、人材不足——経営アジェンダと隔たり

多様化するリスクを多角的な評価軸で十分に評価できていないという実態は、サプライチェーンリスク管理の矮小化^{わいしょう}にもつながります。

リスク管理の検討機会について、最も多いのが「各関係部門の会議体で定期的に検討を実施している」(44%)でした(図表4)。一方で、「取締役会など経営層が出席する会議体で定期的に検討を実施している」と回答したのは35%。さらに、「問題が発生した際に個別に検討を行っている」という事後対応的な回答も35%に上りました。

図表4：サプライチェーン全体のリスク管理の検討機会

Q. 貴社におけるサプライチェーン全体のリスク管理の検討状況として、あてはまるものをお選びください。



出所：PwC作成



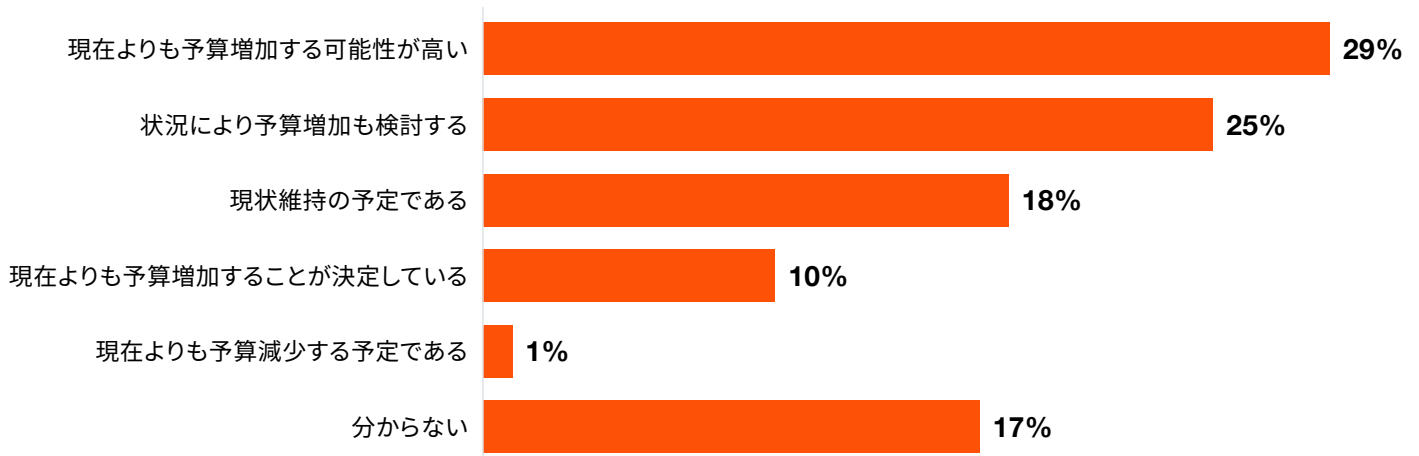
こうした結果から、リスク管理が全社的な経営会議の定期的な議題として検討されるのに比べ、関係部門レベルで検討される方が相対的に多いという傾向が見られました。そのため、部門最適の議論に終始し、全社横断での戦略的なリソース配分や、中長期的な投資判断がなされにくい構造が、対策の遅れを助長していると考えられます。

実際、今後必要な対応として最も多く挙げたのは、「人的リソース・体制の増強」(43%)でした(図表6)。また、調査対象の288社はいずれも売上高100億円以上ですが、サプライチェーンリスク管理への投資金額について143社が1億円未満と回答。今後3年間の予算額についても、「増加を決定」と「増加の可能性が高い」の合計は39%にとどまり、約6割が現状維持や状況次第とするなど消極的な姿勢が目立ちます(図表5)。

仮に供給網が麻痺すれば、事業活動が広範囲にわたって停滞し、業績に大きなダメージをもたらす恐れがあります。また、顧客や取引先にも悪影響が及びかねず、社会的な問題にまで広がれば自社のブランドが大きく傷つくでしょう。想定される影響の大きさを踏まえると、人員・投資規模の妥当性を再検討する余地があります。

図表5：サプライチェーンリスクマネジメントに対する投資予算見通し

Q. 貴社のサプライチェーン全体のリスク管理に対する今後3年間の投資予算額について、最も近いものをお選びください。



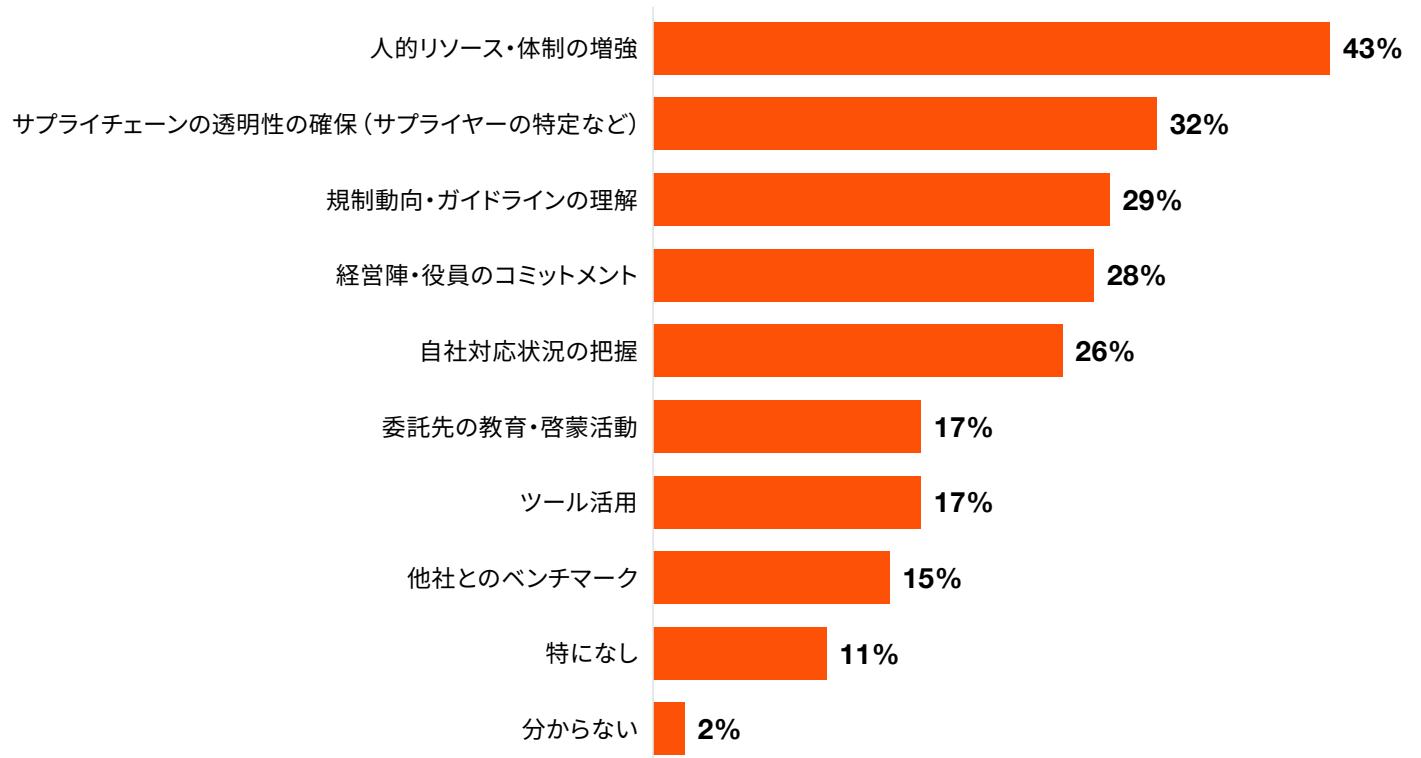
出所：PwC作成

投資額について言えば、「災害」や「サイバー」といった個別領域の対策はきちんと行っているものの、それらをサプライチェーン管理のカテゴリーに含めていないために金額が少なくなっている可能性も考えられます。ただ、それもサプライチェーンリスク管理を統合的に捉えていないことの裏返しと言えるでしょう。

部門主導、限定的な投資、人材不足——。これらの課題は、サプライチェーンリスク管理を全社的な経営課題として位置づけ、資源配分を検討する必要性を示しています。サプライチェーン管理を経営アジェンダに設定し、全社的な戦略の下でヒト・モノ・カネといった経営資源を適切に配分することが、強靱化への第一歩となります。

図表6：サプライチェーンリスクマネジメント推進における課題

Q. 貴社におけるサプライチェーンリスク対応で、(現在対応が不足しており) 対応が必要と考えるものは何ですか。



出所：PwC作成

デジタル活用は進むも 見えぬ供給網に半数が不満

「サプライチェーンの全体像が把握できない」。多くの企業で、こうした悩みを聞きます。サプライチェーンリスクがやっかいなのは、自社の対応が万全であっても、長く連なる「鎖」のどこかで生じたほころびが、全体に影響を及ぼしかねない点です。

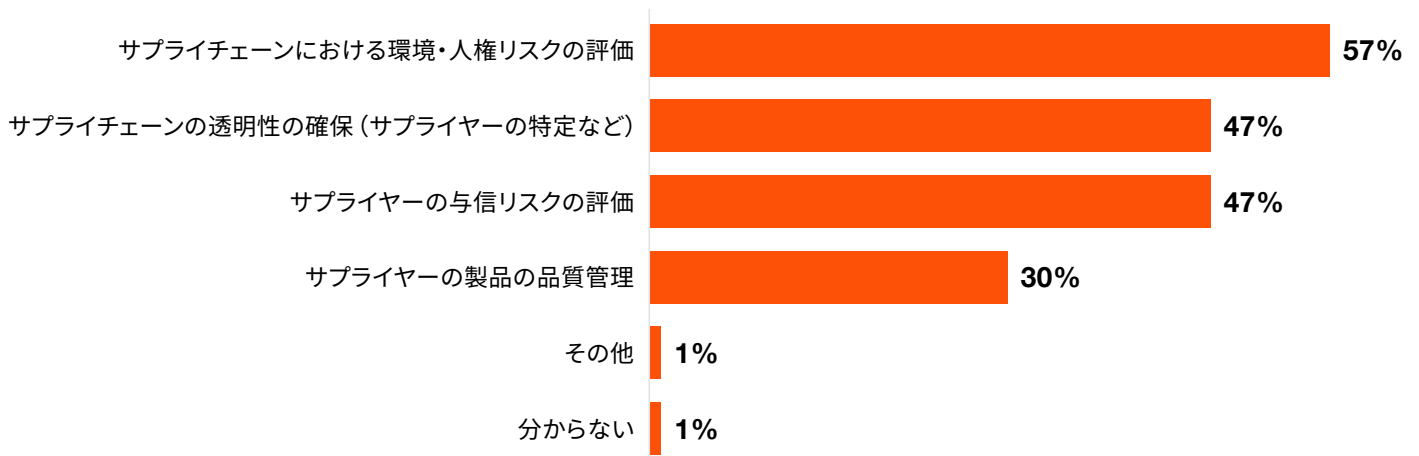
ただ、供給網は地域や国境を越えて重層的に広がっているため、全容を把握して情報を更新し続けるのは至難の業と言えます。特に鬼門となるのがTier2(2次取引先)以降の情報の可視化です。自社からは見えづらいうえに、地政学やESG関連のリスクを見過ごす恐れがあります。また、直接的な契約関係がない企業ともなれば、データの収集と集約をしようにも時間と労力がかかるでしょう。

こうした課題の解決に向けては、デジタルツールとデータの活用が欠かせません。実際、導入は進んでいるようです。デジタルツールの具体的な用途として、「サプライチェーンにおける環境・人権リスクの評価」(57%)が最も多く、「サプライチェーンの透明性の確保(サプライヤーの特定など)」(47%)と「サプライヤーの与信リスクの評価」(47%)が続きました(図表7)。

供給網の可視化だけでなく、与信や品質といった従来のサプライヤー管理、そしてESGを含む非財務リスクの評価にも、デジタルツールの活用が拡大しています。より複雑で社会的な要請が強い領域にまで企業のリスク管理の対象が広がる中、対応手段としてデジタルツールやデータの存在感が高まっていることを示しています。

図表7：デジタルツールの用途

Q. デジタルツールはどのような用途で活用していますか。



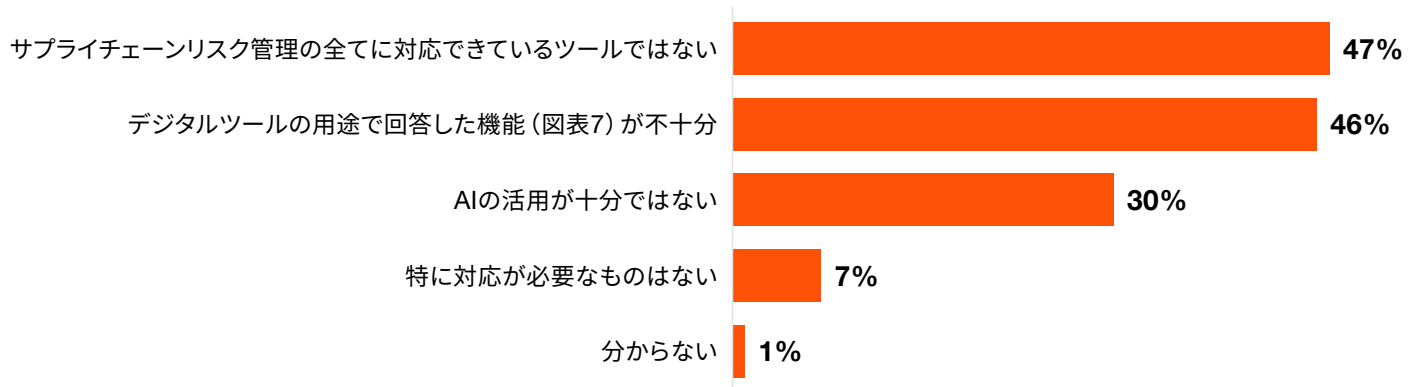
出所：PwC作成

それでもなお、今後必要な対応として「サプライチェーンの透明性の確保(サプライヤーの特定など)」(32%)が課題の上位に挙がっており、ツールを活用しても満足のいく可視化につながらないというジレンマがうかがえます(図表6)。

その原因として「サプライチェーンリスク管理の全てに対応できているツールではない」(47%)、「現在ツールを活用している用途に関する機能が十分ではない」(46%)、「AIなどの最新技術の活用が十分ではない」(30%)といったツールの機能に限界を感じている状況が、調査の結果から浮かび上がりました(図表8)。

図表8：デジタルツールにおいて現在対応が不足しているもの

Q. 利用しているデジタルツールについて(現在対応が不足しており)対応が必要と考えるものは何ですか。



出所：PwC作成

これらの結果を総合すると、取引先の末端(Tier N)までを可視化し、サプライチェーン全体で起こり得る多様なリスクを一元管理できる状況には至っていない企業が多いことが分かります。特にTier2以降のサプライヤーに起因する「サイバー」「ESG/環境」「地政学」といった脅威を事前検知できない恐れがあり、仮に問題が発生すれば受け身で対応せざるを得ない状況に陥るでしょう。

現状でこうした問題を完全に解決できる「魔法の杖」のようなツールは存在しないかもしれませんが、できることはあります。例えばAIエージェントを活用することで、企業の公表資料から主要な取引先の情報を集められます。また、異常気象や災害の発生情報とサプライヤーの立地場所を踏まえて、供給が止まりそうだというアラートを受け取ることも可能です。公開情報を機動的に活用できる体制を構築するだけでも情報感度は大きく高まるでしょう。

サプライチェーン管理では把握した取引先の情報を随時更新していくことが大きな障壁となるため、自社のシステムと連携して自動もしくは極めて手軽な作業で情報をアップデートし続けられる仕組みも役立ちます。全体を俯瞰し、リスクの予兆を捉えるための「目」となるデータ基盤の構築やAIの活用が欠かせません。

高まる規制・技術の壁——外部専門家起用も 活用範囲は限定的

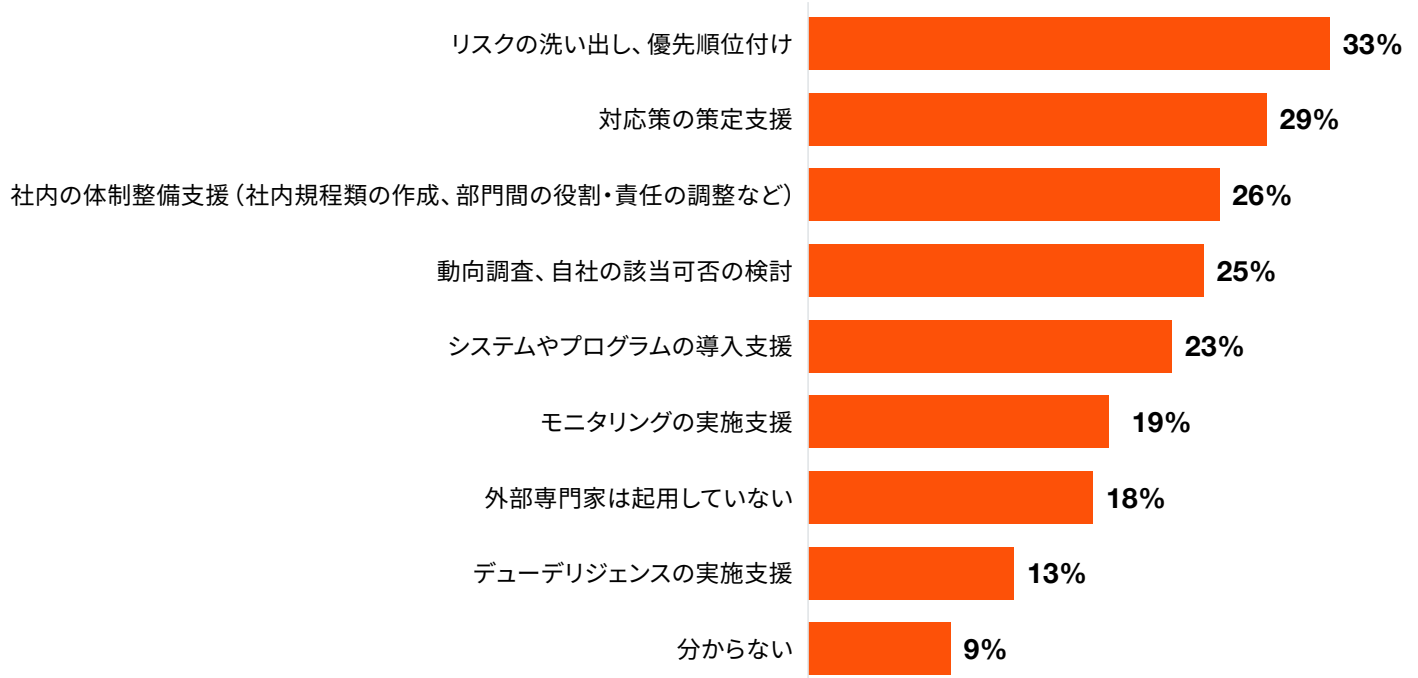
環境や人権を巡る法規制が複雑化する中、多くの企業が「どこまで対応すればよいのか」「自社にどれだけの影響があるのか」といった点に頭を悩ませています。調査においても、今後必要な対応として「規制動向・ガイドラインの理解」が3番目(29%)に挙がりました(図表6)。

法規制だけではありません。テクノロジーの急速な進展によって、サイバーセキュリティや品質管理などといった領域でも、高度なデジタルの技術や知見が求められます。さまざまなリスクごとに専門性を求められる場面が増えていると言えるでしょう。多くの企業が人的リソースの不足に悩んでいることには既に触れましたが、人数だけではなく知見やスキル、専門性といった質の面も含めて人材が足りていない状況がうかがえます。

現実的な解決策の1つは外部の専門家を活用することでしょう。調査においても何らかの形で外部専門家を活用している企業の割合は約7割に上ります(図表9)。

図表9：外部専門家の活用状況

Q. 貴社におけるサプライチェーンリスクへの対応について、外部専門家の活用状況であてはまるものをお選びください。

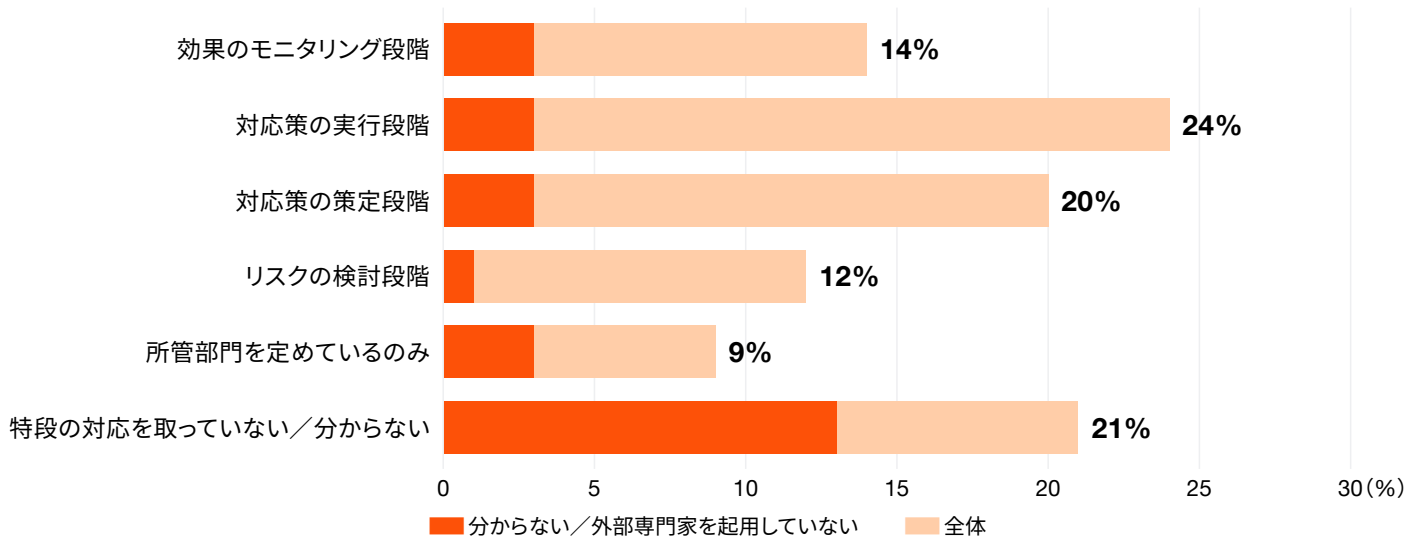


出所：PwC作成

一方、外部専門家を起用していない企業では、全てのリスクにおいて対策が相対的に遅れていることが分かりました。図表10の濃いオレンジ色は、図表9で外部専門家について「起用していない」(18%)、「分からない」(9%)と回答した企業の合計を表しています。全てのリスクにおける対応状況では、全体の回答(薄いオレンジ色)の傾向と比べて、「特段の対応を取っていない／分からない」の割合が明らかに高くなっています(図表10)。

図表10：全てのリスクにおける対応状況

Q. 貴社におけるサプライチェーンリスクへの対応状況について、それぞれ最も近いものをお選びください。



注) 12のリスクに対する回答の合計、複数回答
 出所：PwC作成

ただ、外部専門家の活用範囲はまだ限定的です。図表9では「リスクの洗い出し、優先順位付け」(33%)、「対応策の策定支援」(29%)、「動向調査、自社の該当可否の検討」(25%)といった、調査・分析から計画策定にかけてのフェーズが多くなっています。これらと比較すると、「モニタリングの実施支援」(19%)や「デューデリジェンスの実施支援」(13%)など、実行・定着フェーズにかかわる領域での活用は少ない傾向にあります。

多くの企業が、スポット的な情報収集やアドバイスを得るための「調査委託先」として外部専門家を捉えており、サプライチェーンリスク管理の戦略策定から実行、定着までを一貫して伴走する「戦略的パートナー」として活用するには至っていない傾向がうかがえます。

最も大切なことは調査・分析による状況の把握だけではなく、その先の戦略策定、そして実行と定着です。特に環境や人権、経済安全保障やサイバーセキュリティなどの領域では、最新の動向を読んだ上で、高度な知見をどうやって組織に体系立てて落とし込むかといったプロセスが欠かせません。自社で対応できる部分やするべき部分と、外部の専門家を活用して知識や時間を「買う」部分を分けて対策を進めることが、リスク管理の速やかな高度化につながるでしょう。

強靱なサプライチェーン構築に向けた5つの変革

多様なリスクが企業を取り巻く中、サプライチェーンの危機管理に対する意識や対応が追い付いていない実態が、本調査を通して浮き彫りになりました。その根本にある構造的な課題を解消し、真に強靱なサプライチェーンを構築するには何に取り組むべきでしょうか。処方箋として、以下の5つの変革を提言します。

1. 縦割りからの脱却

全社横断のリスクフレームワーク構築を

個別リスクごとの縦割り管理から脱却し、サプライチェーン全体のレジリエンス向上を目的とした統合的なフレームワークの構築が急務です。現状は人事労務や調達など、部門ごとに個別リスクに向き合う企業が目立ちます。このままでは正しいリスク像が経営陣に伝わらず、重要性が過小評価されて現場任せになり、投資も人材補充も行われないう悪循環に陥ります。社内情報を速やかに吸い上げ、経営陣が俯瞰的に物事を判断できる横断体制の構築が欠かせません。

2. 多角的なリスクへの対応

非財務の観点を含む評価軸設計が急務

売上や事業継続への影響額など、比較の見積もりやすい要素に重きを置いたリスク評価は、潜在的ながらも深刻な影響を及ぼし得る非財務領域のリスクを見過ごす危険性をはらみます。ブランド価値、顧客からの信頼といった定性的な要素と、想定損失額などの定量的な要素を組み合わせ、多角的なリスクに対応する評価軸を急ぎ確立する必要があります。

加えて、人権や環境リスクは、自社が受ける影響だけでなく、ステークホルダーが被る影響を評価する仕組みの構築も重要です。投資家やサプライチェーン上の労働者はもちろん、地域住民、生態系や自然・生活環境などに対し、自社の引き起こす人権・環境リスクがどの程度の深刻さと範囲で影響し得るのかを、体系的に把握・評価する必要があります。それによって真に対応すべきリスクが可視化され、経営陣はよりの確な判断を下せるようになるでしょう。

3. 不足する専門性は外部知見で補完 体制構築・人材育成まで見据えた活用を

環境や人権関連の規制が複雑化し、テクノロジーも急速に進展する状況において、自社の人材で全てのリスクに対応しきるのは至難の業です。外部の専門家を起用して、人的リソースを質と量の両面で補う必要があるでしょう。

その際、調査・分析にとどまらず、戦略策定から体制構築、実行・モニタリングまで一貫して伴走を求めることで効果は高まります。外部知見を組織に取り込むことができれば、人材の育成にもつながり、中長期的には自社の対応力そのものも底上げされるでしょう。自前の人材が専門性を吸収し、将来的には自走できる体制を築くことも視野に入れるべきです。外部人材の活用を一時的な「助っ人」起用ではなく、組織能力を高める機会と捉える発想が欠かせません。

4. Tier2以降の「見えない鎖」 AI・データ基盤で可視化

Tier1に加え、Tier2以降のサプライヤーや物流事業者を含め、サプライチェーン全体にまでリスク管理の対象を拡大し、透明性を確保する必要があります。起こり得る多様なリスクを一元的に可視化するには、AIなどを活用した次世代の統合プラットフォームの導入が欠かせません。同時に、バリューチェーン全体のリスク情報をリアルタイムに把握・分析するデータ基盤の構築も求められます。

主要または潜在的リスクの高い製品・サービスについては、関連するサプライヤーや拠点を特定します。その上で評価したリスクに応じて対策を講じ、ツールを通して継続的にモニタリングするプロセスを仕組み化できれば実効性が高まります。

サプライチェーンは脆弱な部分からほころびが生じるため、取引先における意識向上や対策強化も併せて、全体の防御力を高めていくことが肝心です。ただ、サプライヤーによって資金面・人材面での体力や自社にとっての重要性は異なります。一律ではなく、優先度合いに応じた対策の実施を促す必要があるでしょう。

5. 部門主導から経営主導へ トップのコミットメントが強靱化の鍵

不確実性の高い時代において、サプライチェーンリスク管理は各現場で対処すべきものではありません。インシデント発生後の個別対応といった受け身の姿勢を含め、現場任せの状況を早期に脱却する必要があります。

鍵を握るのは、経営陣のリーダーシップです。サプライチェーンリスク管理を経営アジェンダの1つと位置づけ、全社的な戦略と中長期的な投資計画を策定・実行できるかが問われます。レジリエンスの向上を競争力の強化と捉え、積極的にリソースを配分する経営判断が求められます。

複合リスク時代こそ供給網は「生命線」 経営陣のリーダーシップが強靱化の鍵

サプライチェーンを取り巻くリスクが複雑化する一方、多くの企業で、リスク認識が十分な対策や投資につながっていない状況が見られます。リスクを認識しつつも、具体的な対策や投資に踏み出せない状況から脱却するには、リスク管理のあり方を根本から見直す経営変革が欠かせません。鍵を握るのは、経営陣の危機感と強力なリーダーシップです。

サプライチェーンリスク管理の高度化は、単に損失を回避するための「守り」の活動ではありません。不確実性の高い時代においても安定した事業運営を可能にし、顧客からの信頼を勝ち取って、新たな事業機会を創出する「攻め」の経営戦略です。サプライチェーンは企業の「生命線」であり、その強靱化は持続的な成長を支える最も重要な経営基盤の1つとなるでしょう。

ここまではサプライチェーンリスク管理における日本企業の現在地と、取り組むべき施策を概観してきました。次の章では、調査の中でも企業が強い懸念を示し、実際に影響を受けた割合も高く、今後の企業運営においても重要と見られる主要なリスク(災害、品質、サイバー、ESG/環境/人権/労務)の分析と対策を提示していきます。



供給網を蝕む4つの脅威 ——領域ごとの実態と企業が取べき対策

ここまでの調査結果と提言では、サプライチェーンリスク管理の全体像を俯瞰し、日本企業を取り組むべき5つの変革の方向性を示しました。ただ、リスクの性質は領域ごとに大きく異なります。自然災害やパンデミックといった不可抗力によって供給網を物理的に寸断する「災害」、製品やサービスの信頼を根底から揺るがす「品質」、デジタル化の進展に伴いサプライチェーン全体に瞬時に波及する「サイバー」、そして規制強化やステークホルダーの目が厳しさを増す「ESG／環境／人権／労務」——。いずれも企業にとって対策の重要性が高い領域でありながら、求められる専門知識や管理手法、そして直面する課題はそれぞれ異なります。

本調査でも、これらのリスクは懸念・影響の割合が一定程度高く、今後の規制・事業継続・社会的要請の観点からも対応の重要性が高い領域です。以降の章では、各領域の最新動向や調査から見えた企業の課題を掘り下げるとともに、実効性のある対策を提示します。全体を通じた提言と、個別領域ごとの具体策を重ね合わせ、自社のサプライチェーンリスク管理を点検・強化するための実践的な指針としてご活用ください。

災害

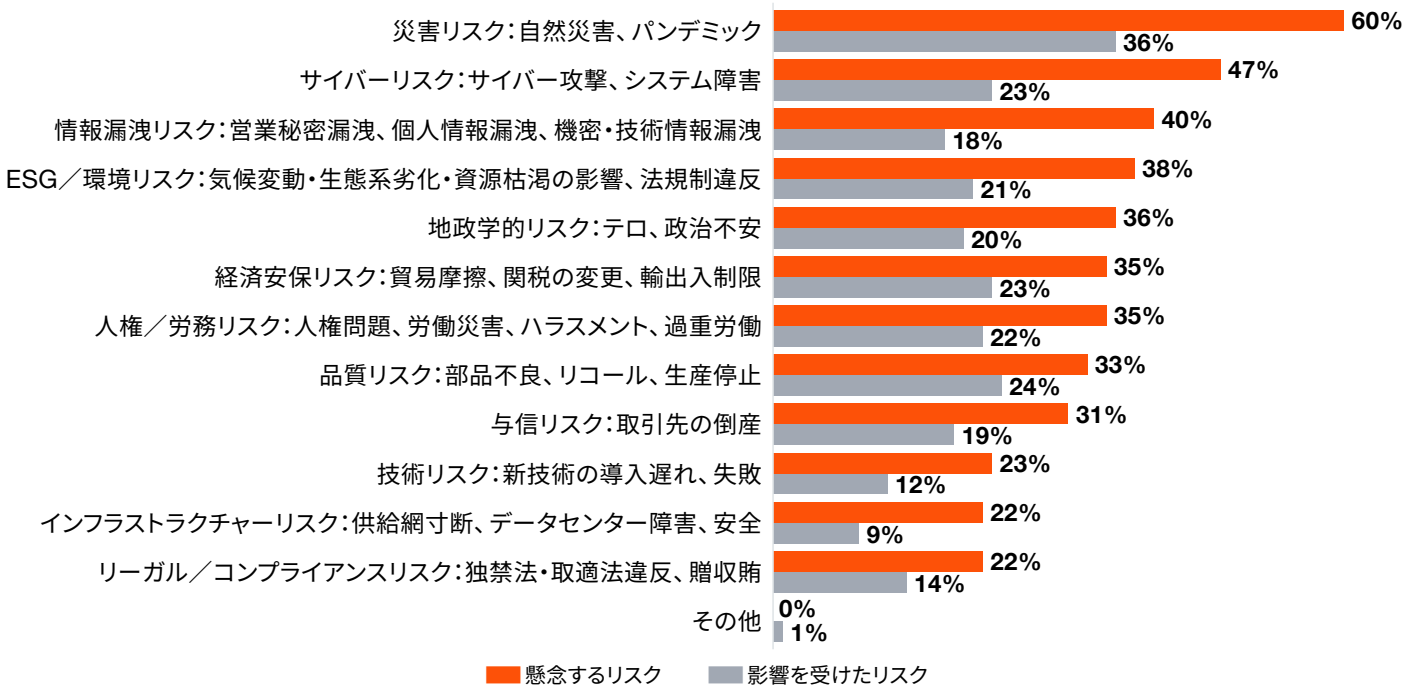
「備えている」は本当か 気候変動時代の災害対応を再評価する

地震や台風、洪水などが頻発する日本において、企業がサプライチェーン上の最大の脅威として捉えているのがパンデミックを含む災害です。今回の調査でも、60%の企業が災害を懸念しており、36%の企業は実際に影響を受けたと回答しています。懸念・影響ともに12のリスクの中でトップでした(図表11)。

それだけに他のリスクに比べて対応も比較的進んでいることがうかがえます。対応策について、「実行段階」もしくは「効果のモニタリング段階」と回答した企業は計47%に上りました(図表2)。これも全てのリスクの中で最も高い数値です。

図表11：懸念するリスクと影響を受けたリスク(再掲)

Q. 貴社が懸念するサプライチェーン上のリスクおよび実際に影響を受けている／過去に影響を受けたリスクは何ですか。



出所：PwC作成

しかし、気候変動の進行に伴い、従来の想定を超える災害が増加する可能性があります。サプライチェーンが複雑化していることを考慮すると、局地的な災害であっても、企業活動全体に甚大な影響を及ぼしかねません。一見すると災害への備えは進んでいるように見えるからこそ、対策の実効性を厳しく再評価すべき段階になっているのではないのでしょうか。

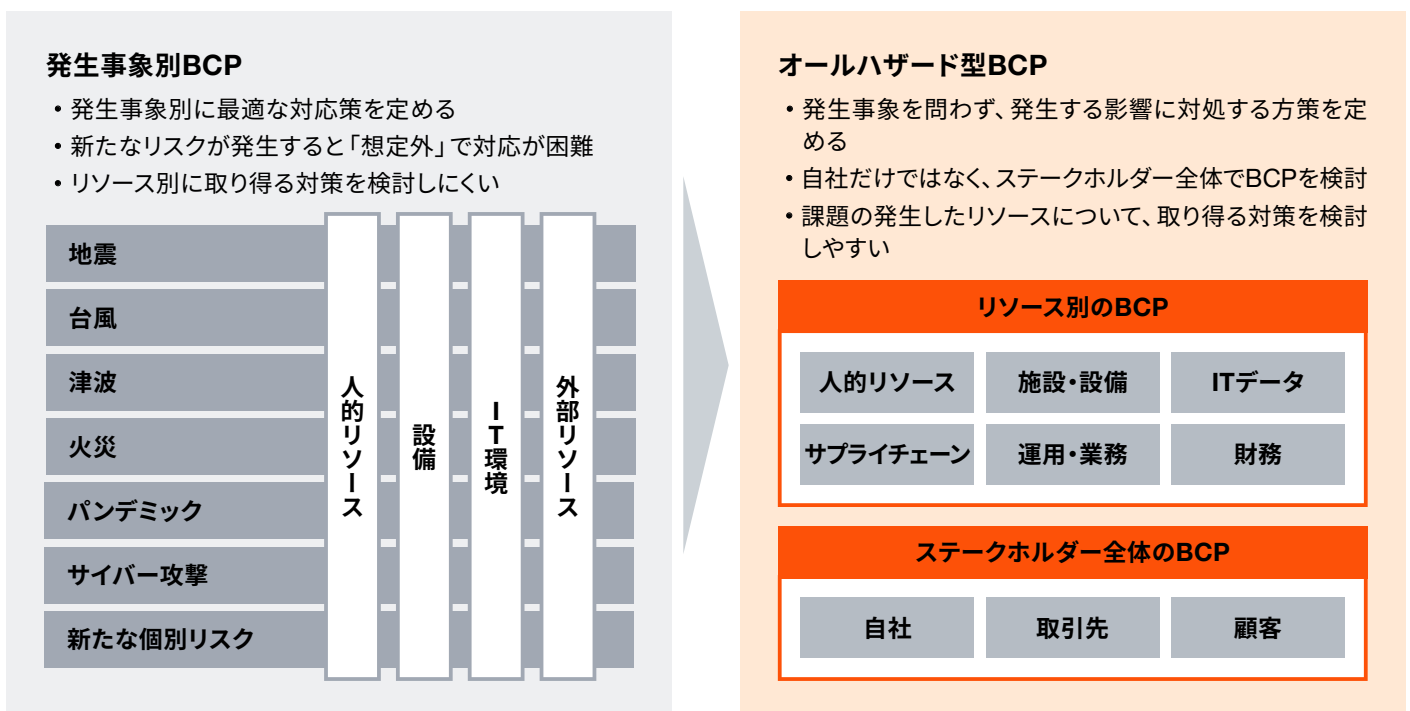
災害別BCPの限界 「原因別」から「影響別」への発想転換

多くの企業の災害対応を詳細に見ると、ある共通した課題が浮き彫りになります。それは「地震」「台風」「パンデミック」といった災害事象ごとに個別のBCPやマニュアルが策定されているという点です。このアプローチは一見丁寧に映りますが、実際の運用上は多くの無駄と混乱を生み出しかねません。

例えば、地震と台風では、「従業員の安否確認」「ITシステムの復旧」といった必要なアクションには多くの共通項が存在します。しかし、これらを縦割りのマニュアルとして個別に管理すると文書が膨大化し、有事の際に「どのマニュアルのどこを見ればよいのか分からない」という事態につながります。

こうした「個別最適」の罫から脱却するために重要なのが、発生事象（地震か台風か）ではなく、影響事象（企業の機能に何が起きたか）に着目する「オールハザード型BCP」への転換です（図表12）。具体的には、「電力が止まった」「物流が途絶えた」「従業員が出勤できなくなった」といった「影響」をベースに対策を講じる考え方を指します。

図表12：オールハザード型BCPの概要



出所：PwC作成

原因が何であれ、影響が同じであれば、とるべき対策は共通化できます。その結果、膨大なマニュアルを一本化・シンプル化することが可能になり、有事の際の意思決定スピードを高められるでしょう。また、このアプローチは災害だけでなく、サイバー攻撃や地政学リスクなど、将来発生し得る未知のリスクに対しても有効であるため、組織の基礎的なレジリエンスの向上につながります。

自社の全体像をデジタルで把握 資産・商流の可視化が対策の起点に

実効性のある対策を打つための大前提となるのが、自社の現状を正確に把握することです。しかし、多くの企業では、どの地域にどのような資産（工場、在庫、人員）があり、それがどのサプライヤーや顧客とつながっているのかという全体像について、リスク管理の観点から十分に可視化できていません。

自社の備えを他社の備えにも 共助で実現するサプライチェーンの強靱化

自社の体制が整ったとしても、サプライヤーが被災し部品や素材の供給が止まれば事業は継続できません。構築したリスク可視化の仕組みや対応計画は、自社内にとどめるのではなく、主要なサプライヤーとも共有し、対応方針をすり合わせておくことが重要です。

「有事の際にはこう動く」という認識を平時から共有し、Tier2以降も含めたサプライチェーン全体での共同訓練や情報連携を行うことで、レジリエンスが高まるでしょう。

平時の柔軟性が有事を救う 日常のオペレーションに宿るレジリエンス

災害とは、いわば「環境の変化量が極端に大きくなった状態」と捉えることができます。優れたレジリエンスを持つ企業は、災害時にだけ特別な動きをするのではなく、平時から需要の急な変動など日常的に起こり得る「小さな変化」に対して、柔軟に物流や生産を調整できる仕組みを整えています。例えば、ある地域で需要が急増し、あらかじめ設定した閾値^{しきい値}を超えた場合、即座に他拠点からの輸送に切り替えて供給を補うといった対応です。

日常的にこうした変動に対応できていれば、その変化量が極大化した「災害」が起きた場合でも、同じ仕組みを基盤として、より迅速に対応できます。逆に、平時の小さな変化にすら柔軟に対応できていない組織が、災害という極限状態においてのみ適切に動くことは困難でしょう。

日々のビジネスにおける変化への感度を高め、それに対応する無駄のない機動的なオペレーションを構築しておくことが、結果として巨大地震などの「大きな異変」への対応力を養うことにつながります。BCPを単なる「非常時のマニュアル」として形骸化させるのではなく、日々のサプライチェーン最適化や経営判断の中に組み込んでいく姿勢が問われます。



品質

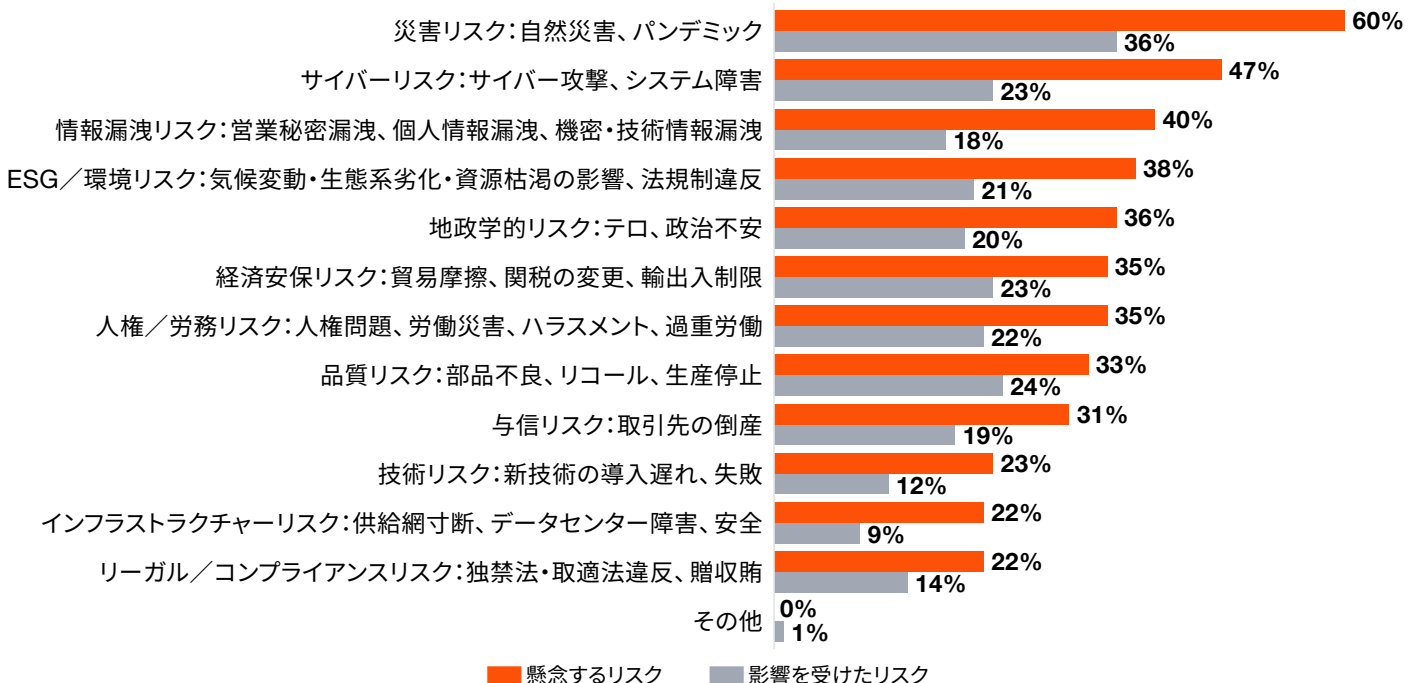
「管理する」から「共に高める」へ 品質を支える信頼の連鎖

サプライチェーンが世界に広がり複雑さを増す中で、製品やサービスの品質を維持する難易度は格段に高まっています。今回の調査では、3割以上の企業がサプライチェーン上の懸念に品質リスクを挙げ、実際に影響を受けた企業も2割台に上りました(図表13)。ただ、品質リスクの原因は発注元である自社に起因するケースも見られます。供給網が複雑さを増す状況だからこそ、真の問題がどこに潜んでいるかを見返す必要があるでしょう。

ここでは、品質リスクの要因を受発注双方の構造から分析した上で、サプライヤーの重要度に応じた管理設計を起点にした5つの打ち手を提示します。根底にあるのは、サプライヤーを「品質管理の対象」から「品質を共に高めるパートナー」へと捉え直す発想の転換です。

図表13：懸念するリスクと影響を受けたリスク(再掲)

Q. 貴社が懸念するサプライチェーン上のリスクおよび実際に影響を受けている／過去に影響を受けたリスクは何ですか。



出所：PwC作成

見落とされる「自社起因」——発注元が生む品質リスクの構造

供給網上の品質問題に対し、多くの企業はサプライヤー管理の強化に目が向きがちです。しかし、発注元である自社の調達行動や体制が品質リスクを発生・増幅させる温床になっていないかを、まず問うべきでしょう。品質問題に直結する4つの典型的な要因を概観します。

1. 過度な要求

コスト削減率を主要な評価指標として課された調達部門は、一方的なコストダウンや短納期を要求しがちです。それが常態化すれば、サプライヤーは品質より納期や価格を優先せざるを得なくなり、問題に発展しかねません。インフレ基調が強まる中、特に目を光らせる必要があるでしょう。取引実績のない企業に、既存サプライヤーと同等の水準を画一的に求めることも思わぬリスクにつながります。根本には、過度な要求が製品の品質を劣化させ、事業継続を脅かすという認識が組織内に浸透していないことがあります。

2. 品質要求の不十分な伝達

仕様書や図面の記載が曖昧で、「どの特性を、どの水準で、どう検査するか」が明文化されていなければ、サプライヤーごとに品質基準の解釈にばらつきが生じかねません。サプライチェーンの階層が深くなるほど、品質要求が伝言ゲームのように劣化するリスクが高まります。特に製造業では、従来の機械部品中心の品質管理から電子制御やソフトウェアも含めた複合的な品質保証へ対応領域が広がり、サプライヤーとの意思疎通の難易度は格段に上がっています。

3. 部門間のサイロ化

設計・調達・製造・品質保証の各部門が個別に動く組織では、設計部門がサプライヤーの製造能力を考慮せずに仕様を確定し、調達部門はコストと納期だけを交渉、品質保証部門は問題発生後に初めて関与するといった分断が起きやすくなります。これでは品質リスクが「誰の責任でもない領域」に押しやられ、サプライチェーン横断のガバナンスは機能しません。海外の拠点やサプライヤーとの連携が日常となった今、この縦割り構造は国境を越えた情報の分断を引き起こし、死角をさらに広げます。

4. サプライヤーの選定・検証プロセスの不備

選定基準が価格と納期に偏り、品質管理体制の評価が後回しにされたまま取引が始まるケースは珍しくありません。そうした状態に受入検査の簡略化や品質監査の形骸化が重なれば、品質問題が顕在化するまでリスクは水面下に潜り続けます。

重層化する供給網の死角——サプライヤーに内在するリスク

次に、サプライヤー側が抱える品質リスクの要因を見ていきましょう。さまざまな状況変化を受けて、以前から存在する課題がより根深いものになっていることが分かります。

1. 「見えない領域」の広がり

Tier1からTier2以降に製造が再委託される過程で、階層が深くなるほど品質管理の実態が不透明になります。Tier1がTier2以降を適切に管理していたとしても、その先の品質体制が脆弱であれば蟻の一穴となるでしょう。

Tier2以降の品質管理の実態が見えにくいという課題はこれまでもありましたが、取引構造の分断によって情報が伝達されにくくなり、品質管理責任が曖昧化する傾向がより強まりました。情報開示水準やIT基盤が各社で統一されておらず、デジタル化への対応が遅れている中小事業者の多さも、供給網の死角になります。

2. 供給網の再編・拡大

地政学リスクの高まりと経済安全保障の観点から、フレンドショアリングなどによるサプライチェーン再編の動きが広がってきました。こうした中で品質のばらつきを生みやすいのが、国や地域ごとに異なる品質基準・規制・商習慣です。新規サプライヤーは品質管理手法やものづくりの文化などが既存取引先と異なる場合が多く、より入念な監査や指導が求められます。

3. リソース制約

品質管理に投下できる人材、設備、資金には限りがあります。発注元がいくら高い品質水準を要求しても、サプライヤー側にそれを実現する経営体力がなければ、要求は形骸化するか、無理な対応による別のリスクを生むでしょう。高度技能人材の不足や熟練技能者の高齢化で、製造現場や品質管理を支えるリソースが限られることも、こうした状況に拍車をかけています。

4. 原材料・部素材の変動

サプライヤーにおける調達先の切り替えに伴って起こり得るリスクもあります。原材料の産地やロットが異なることで加工条件が微妙に変化し、製品の品質に影響を与えることがあるためです。地政学リスクや経済安全保障を理由に調達網を見直す可能性が高まっているだけに、注意を払う必要があるでしょう。

管理から協働へ——品質リスクに向き合う5つの打ち手

上記の構造的要因を踏まえ、発注元の企業が取るべき具体策を5つ提示します。全てのサプライヤーを一律に管理するのではなく、重要度に応じた濃淡をつけ、各打ち手をどの層に、どこまで適用するかを明確にすることが重要です。

打ち手1 一律管理からの脱却 リスクに応じた濃淡設計

品質リスクの要因は多岐にわたり、全てに同一レベルの対策は講じられません。まずは以下の観点で、サプライヤーの重要度に応じた管理レベルの設計に着手すべきです。

- 取引規模：取引金額(年間購買額)、取引量の大きさ
- 事業影響度：供給断絶時の事業影響の大きさ(生産停止の可能性・売上損失)と影響範囲
- 供給部品の重要度：最終製品の安全性・性能に直結する部品
- 代替調達の困難さ：特殊技術を要し、代替が困難な部品
- サプライチェーン上の位置と可視性：Tier2以降で実態が見えにくいサプライヤー
- 過去の品質実績と経営環境の安定性：品質事故履歴、M&A、財務状況の推移

この分類に基づき、以降の打ち手2～5の適用範囲を図表14のように設計します。まずは売上高や部品の安全性への影響度といった既存データで簡易スクリーニングをし、上位20%の重要サプライヤーの特定から始めるなど、完璧な分類ではなく「濃淡をつける」という意思決定が重要です。

図表14：サプライヤーの分類条件と適用する打ち手

レイヤー	対象サプライヤーの特徴	適用する打ち手	管理の考え方
管理レベル A (最重要)	安全性・性能に直結する部品を供給／ 代替困難／品質事故の影響が甚大	打ち手2～5を全て適用	品質ガバナンスへの組み込み、データ連携、定期的な品質対話、共同監査を全面的に実施
管理レベル B (重要)	重要部品だが代替可能性あり／品質のばらつきに注意が必要	打ち手2・5を中心に適用。打ち手3・4は重点テーマに絞って適用	ダッシュボードによるデータモニタリングとリスクベースの監査を軸とし、必要に応じて品質対話を実施
管理レベル C (標準)	汎用部品を供給／代替が容易／品質実績が安定	打ち手3を主軸に適用	セルフアセスメントと受入検査データのモニタリングを中心に、異常検知時にのみ深掘り対応

出所：PwC作成

打ち手2 縦割りを超える——品質ガバナンスの横断的構築

品質リスクの多くは、設計・調達・品質保証の各部門が個別に動き、サプライチェーン全体を横断した品質ガバナンスが不在であることに根ざしています。サプライヤーへの品質要求の「策定→伝達→検証」を一気通貫で管理する横断的な仕組みの構築が欠かせません。

策定段階

設計部門が仕様を確定する際に品質保証・調達部門が早期に参画し、サプライヤーの製造能力での実現可能性や検査基準の明確性を検証するプロセスを制度化します。

調達方針決定段階

コスト削減要求や納期設定の妥当性を、品質保証・リスク管理部門を交えて審議し、「この削減目標はサプライヤーの品質維持能力の範囲内か」という問いを経営レベルの意思決定に組み込みます。

検証・フィードバック段階

品質データや監査結果を設計・調達部門にフィードバックし、次の仕様策定や調達方針に反映するサイクルを回します。

調達部門のKPIはコスト削減率に重点が置かれるケースが多く、品質指標を単純に加えようとすると、現場から抵抗感が生まれる可能性があります。こうした意識を変えるには、品質問題に起因するコスト（リコール費用、納期遅延の損害など）を試算・定量化し、経営層や現場に「品質を守ることがコスト削減に直結する」とKPI変更の合理性を示すことが有効です。

打ち手3 品質の「全体像」をデータ集約で浮き彫りに

情報がサプライチェーンの中で分断されて全体像が見えないことは、多くの品質リスクに共通しています。そこで必要になるのが、品質情報の共通フォーマットとダッシュボードです。受入検査や工程内検査の結果、是正処置、変更通知などの情報を一元管理しサプライヤーとも共有した上で、不良率・再発率・是正リードタイムなどのKPIをダッシュボードで可視化。閾値の超過時にアラートが発出される運用を組み込むことで、問題の顕在化前に関係者が察知できる体制を構築します。

サプライヤーが多拠点・多国間にまたがる場合は、重要部品・重要工程を担うサプライヤーを重点対象とし、共通KPIで比較可能な状態を整備。リモート監査やデジタルチェックリストも活用し、限られた負荷で可視性を高めます。運用の定着後は画像判定などの技術を取り入れながら段階的にモニタリングを拡張するとよいでしょう。

サプライヤーごとにITリテラシーやシステム環境に差があるため、共通フォーマットでのデータ収集が思うように進まないケースも考えられます。最初から高度なシステム連携を求めず、最重要と分類する管理レベルAから段階的に導入し、成功事例を横展開するアプローチが現実的です。フォーマット自体の共通化は求めず、収集するデータ項目の共通化を優先する方法も有用でしょう。

打ち手4 価格交渉の先へ 品質対話という仕組み

発注元とサプライヤーの間に横たわる情報の非対称性が、品質リスク蓄積の根本原因の1つです。デジタルツールで定量データの非対称性は縮小できますが、経営判断や組織変化、コスト構造の実態といった定性的な情報は、制度化された対話の仕組みがなければ得られません。

そこで設けるべきなのが、価格交渉と切り離れた定期的な品質対話の場です。双方の経営層や品質責任者が参加し、品質を維持するための納期やコストといったサプライヤー側の実情が率直に共有される仕組みとします。対話軸が「価格交渉」に固定化され形骸化するのを防ぐ上でも、この分離は不可欠です。

コスト削減が必要な局面では一方的な単価引き下げではなく、VA／VE（Value Analysis：価値分析／Value Engineering：価値工学）を通じた、品質を落とさないコスト低減を共同で検討するプロセスも定着させるべきでしょう。

また、M&Aや人員削減、調達先変更といった大きな変化は、製品の品質に波及する前に兆候が表れます。定期的な対話の場は、こうした変化に伴う品質リスクの早期察知にも有効です。

打ち手5 指摘から伴走へ データが変える品質監査の形

品質監査はデジタルデータでは捉えきれない現場の実態を直接確認できる手段ですが、多くの企業では形骸化し、その機能を果たせていません。品質監査を実効性あるプロセスに再設計するには、2つの取り組みが必要です。

まずは品質監査目的の再定義です。不適合の指摘と是正要求が主目的の従来型から、品質課題の共同特定と改善計画の策定を主目的とする形へ軸足を移行。サプライヤーが抱える制約条件を構造的に把握し、改善に向けた支援計画を共同で策定するプロセスとします。

また、データを活用した監査精度の向上も重要です。打ち手3で整備したデータを監査テーマの設定に活用し、異常の兆候が見られた工程を重点的に確認することで、限られた監査リソースを効果的に配分できます。Tier2以降に対しては、Tier1と連携した監査体制を段階的に整備すべきです。

ただ、Tier1と連携しても全てのサプライヤーに深掘り型の監査を行う余力はないでしょう。そこで図表14のサプライヤー管理レベル(重要度)に応じ、打ち手1のセグメンテーションと打ち手3のデータモニタリングを組み合わせます。例えば管理レベルAのうち異常兆候が検知されたサプライヤーにリソースを集中させる一方、管理レベルCはセルフアセスメントの定期回収で状況を把握するなど、メリハリのある配分が必要です。

複合リスク時代の競争力 「信頼の連鎖」が礎に

5つの打ち手が目指すのは、品質に関する情報がオープンに共有され、課題に共に取り組む「信頼の連鎖」の構築です。

リスクに応じた管理の濃淡を設計し(打ち手1)、ガバナンスを横断的に整えて(打ち手2)、デジタルツールで品質を見える化(打ち手3)。さらに、対話で情報の非対称性を埋め(打ち手4)、監査を共同改善プロセスに転換する(打ち手5)。一連の仕組みが機能すれば、受発注者の双方で品質を「共に高める」行動が根付くでしょう。

サプライチェーンは最も脆弱な部分からほころびるからこそ、自社の行動を正してサプライヤーと品質を底上げする地道な取り組みが欠かせません。その積み重ねが、リスクの絡みあう時代を生き抜く確かな礎となるはずです。

サイバーセキュリティ

デジタル化・階層化・グローバル化——三重の構造変化が招くサイバーの脅威

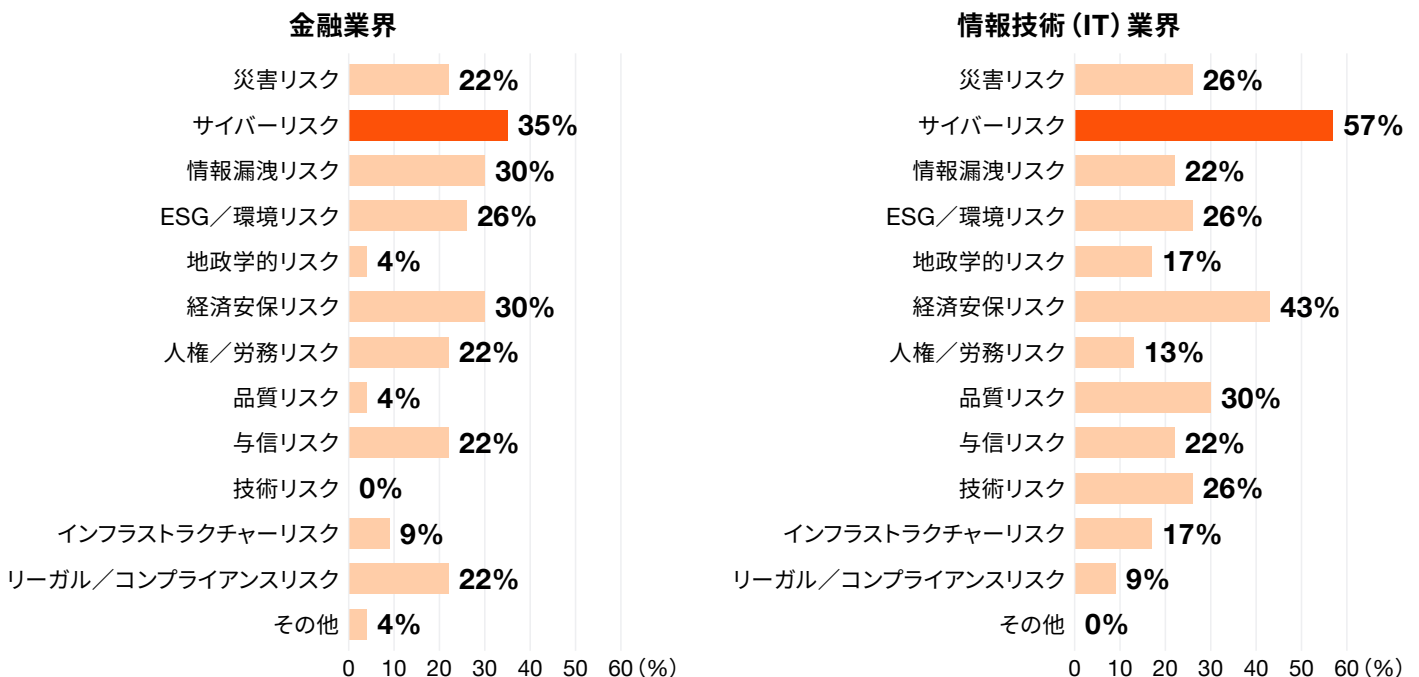
近年、デジタル社会の急速な進展によって企業間のつながりが強化され、企業における責任範囲の境界線を明確に引くことが難しくなっています。サイバー攻撃の手法も高度化・多様化しており、特にサプライチェーン上の企業を狙った攻撃が増えました。サプライチェーンを狙ったサイバーインシデントの増加については、IPA(情報処理推進機構)が発表した「情報セキュリティ10大脅威 2025¹」においても示されており、「サプライチェーンや委託先を狙った攻撃」が第2位に挙げられています。

今回の調査では、「実際に影響を受けている、もしくは過去に影響を受けたサプライチェーンリスク」のうち、「サイバーリスク(例:サイバー攻撃、システム障害)」と回答した企業が、金融業界は35%、情報技術(IT)業界は57%と、他リスクに比べて目立ちます(図表15)。また、アンケートでは実被害を受けた割合は2割台にとどまりましたが、消費者製品・小売業や工業生産(製造業)でも、サイバー攻撃によって甚大な被害を受けるケースが出ています。幅広い業界においてサイバーリスクが大きな脅威になっていると言えます。

その背景には、企業を取り巻くサプライチェーンの「デジタル化」「階層化」「グローバル化」に伴う影響が大きいと考えられます。

図表15：サプライチェーンリスクのうち、影響を受けている／受けたリスク

Q. 貴社が実際に影響を受けている／過去に影響を受けたリスクは何ですか。(金融、技術<IT>)



出所：PwC作成

¹ IPA(独立行政法人 情報処理推進機構), 2025.「情報セキュリティ10大脅威 2025」(2025年6月25日閲覧)
<https://www.ipa.go.jp/security/10threats/10threats2025.html>

1. デジタル化による攻撃面の拡大

IoTやクラウドサービスの導入により、サプライチェーン全体がデジタルで結ばれています。これにより、攻撃者は1つの脆弱な箇所を突破するだけで、広範囲に影響を与えられるようになりました。

2. 階層化による可視性の低下

複数の下請けや外部委託先が関与することで、発注元の企業は全体のセキュリティ状況を把握しづらくなっています。特に中小規模のサプライヤーは、セキュリティ投資が不十分なケースが多く、攻撃の標的になりやすい状況です。

3. グローバル化による規制・文化の違い

国や地域ごとに異なるセキュリティ基準や法規制が存在し、統一的な対策を講じることが難しくなっています。この複雑性が、リスク管理をさらに困難にしています。

限界を迎えた一律・同質なサプライヤー管理

サプライチェーン管理のリスクが高まる一方で、多くの企業が「対応の難しさ」に直面しています。その背景には、以前から一般的に用いられてきた「一律・同質なサプライヤー管理」が要因となっていると考えられます。具体的な問題点は下記のとおりです。

1. チェックリストによる○・×チェックでは実効性が担保できない

現状のサプライヤー管理の方法として多く用いられているのが、企業独自で作成したチェックリストによる評価です。これまで多くの企業では、膨大な数の外部委託先に対して年に一度チェックリストを配布し、受領した回答を用いて管理してきました。

これらのチェックリストでは、サプライヤーに求める各セキュリティ要件について、単純に「○：対策ができていない」「×：対策ができていない」をサプライヤーが自己チェックして提出する形式が大多数であり、「なぜ○と言えるのか」の根拠確認が十分に実施されない傾向にあります。その結果、○・×回答だけのチェックではリスクの本質を捉えることができず、業務自体が形骸化し、労力がかかるだけで本質的なリスク解消に至らないケースが多数発生しています。

2. サプライヤー側の体力(ヒト・カネ)に起因して是正・改善ができない

関係がどれだけ深くとも、子会社でない限りサプライヤーはあくまで独立した企業であり、発注元にとっては「外部の存在」です。サプライヤーは、自社の事業におけるリスクやメリットを勘案の上、自社としての判断でセキュリティ対策を実施するのであり、発注元から対策を「強制」することはできず、「お願い」にとどめざるを得ません。

前提として、日本では、独禁法上の優越的地位の濫用規制に加え、取適法(旧下請法)上の禁止行為にも留意する必要があり、強制と受け取られかねない行為自体を避ける必要もあります。また、外部の企業であるサプライヤーに対策をお願いする際、大企業から中小・零細企業まで多様な規模のサプライヤーが存在する中でコスト負担をどこまで求められるのかという点も、実効的な統制を行う上での難しさとなっています。

総花的管理からの脱却 実効性ある対策への2つの転換

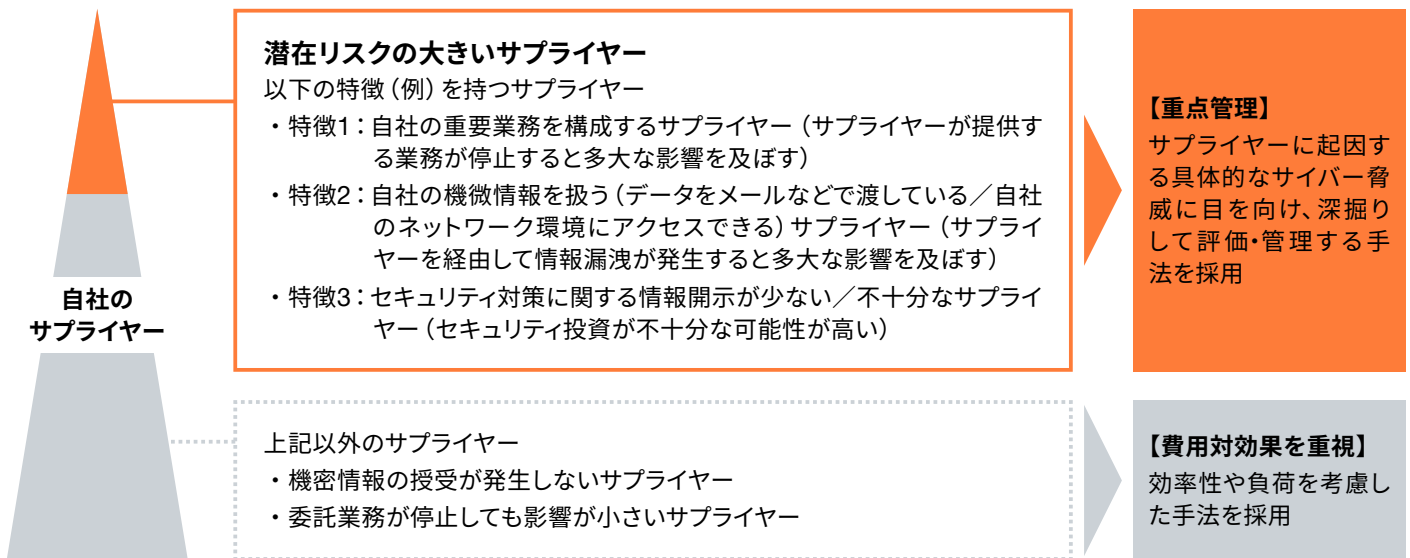
前述した「対応の難しさ」に対し、企業はどのようにサイバーリスクをコントロールすればよいのでしょうか。ここからは、社会・業界全体でデジタルレジリエントなサプライチェーンを確立するためのポイントを解説します。

1. 「リスクベースアプローチ」を取り入れ、実効性を確保する

サプライチェーンリスクの実態を捉えるためには、サプライヤー起因で発生し得る固有リスクに目を向ける必要があります。固有リスクの程度を判断する要素の一例として、「機密情報の取り扱いの程度」「ネットワークの直接接続の有無や接続形態」「再委託の有無」などが挙げられます。

リスクが高いと考えられるサプライヤーに対しては、深度の高い評価・管理でリスクの解像度を上げる一方で、そうでないサプライヤーに対しては相対的に効率性や負荷を考慮した手法でチェックを行うなど、サプライヤーごとに濃淡をつけた評価・管理を行うことが重要です(図表16)。まずは自社における重要なサプライヤー(例:重要業務や重要な部品などを扱うサプライヤー)を定義するところから始め、「総花的・形式的なリスク対応」からの脱却が求められます。

図表16：リスクに応じたサプライヤー評価・管理のあり方



出所：PwC作成

2. 「競争」ではなく「協調」へ

業界・社会全体で最適化された枠組みを構築する

サプライチェーンセキュリティは、自社だけでは完結しません。サプライヤーを含むエコシステム全体で対処が必要です。その際、最も重要になるのは「協調」です。2025年6月に金融庁が公表した「金融分野におけるITレジリエンスに関する分析レポート²」では、「金融機関にとってサイバーセキュリティは、競争分野ではなく協調分野である」と述べられており、当局の考え方がうかがえます。

社会・業界全体でサプライチェーンセキュリティを強固にするためには、国・業界団体による取り組みも必要です。例えば、経済産業省および内閣サイバーセキュリティセンター（現・国家サイバー統括室）では、2024年7月に産業サイバーセキュリティ研究会に「サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ」を設置し、制度構築に向けた検討を開始しました。

本制度は、各企業のセキュリティ対策レベルを「★3～★5」の3段階で業界横断的に可視化することを目指しており、2026年末ごろの運用開始を予定しています。本制度により、受注者側は、自社において一定のセキュリティ対策が講じられていることを客観的に示すことが可能となります。また、発注者側は、適切なレベルのセキュリティ対策が実施されている企業に業務を委託することで、サプライチェーンにおけるサイバーセキュリティの確保が容易になり、発注者・受注者双方のコミュニケーションコストの削減も期待されています。

こうした協調の発想は、業界や国レベルの枠組みにとどまらず、自社とサプライヤーとの関係においても求められます。「一律的なセキュリティ要求リストを用意し、あとは取引先の選定および契約で縛る」といった役割分担論主体のガバナンスは限界を迎えています。取引先に求めるセキュリティ対応について、対策にかかるコストや取引先の体力（ヒト・カネ）を理解し、関係者で合意を取るなどの協調が大切です。

サプライチェーンセキュリティの課題を根本解決するためには、企業・サプライヤーを含むサプライチェーン全体で十分なセキュリティ機能を楽しむことができる枠組みが欠かせません。

リスクの実態・深刻度の見極め欠かせず 実効性ある対策は「協調」から

企業は今、かつてない規模かつ容赦のないサイバー攻撃を受ける危険性にさらされており、サプライチェーンも主要な対象に含まれます。

取引先が攻撃を受けるだけで自社が操業停止に陥ってしまうケースもあり、サプライチェーン全体を意識したリスクガバナンスは経営課題の1つです。これらの課題を解決するためには、総花的なリスク対応ではなく、クリティカルなリスクを見極め、実効性を確保することが重要です。また、業界横断での評価基準の共有や国の制度の活用、さらには取引先の対策コスト・体力を踏まえた合意形成など、「競争」ではなく「協調」の考え方でサプライチェーン全体のセキュリティ水準を底上げしていく姿勢が求められます。

2 金融庁, 2025. 「金融分野におけるITレジリエンスに関する分析レポート」(2025年7月1日閲覧)
<https://www.fsa.go.jp/news/r6/sonota/20250630-2/20250630.html>

ESG／環境／人権／労務

環境・人権デューデリジェンスは「待ったなし」の経営課題

近年、企業のサプライチェーンにおける環境・人権デューデリジェンスの重要性が飛躍的に増しています。その背景にあるのは、気候変動や自然資本の劣化に伴う物理的リスクの顕在化と、環境・人権両面での評判（レピュテーション）リスクの高まりです。いずれも海外で生じた規制や概念が中心のため、どれだけ自社に関係があり、影響を受けるのかを判断しかねる企業も少なくないでしょう。実際は日本企業がいつ巻き込まれてもおかしくない、「待ったなし」の経営課題だと言える状況になりつつあります。

“対岸の火事”では済まぬ環境・人権リスク

環境や人権に絡むリスクが企業経営に影響を与える事例は、もはや珍しくありません。米国ではUFLPA（ウイグル強制労働防止法）施行後、2023年末までに強制労働の疑いで6,315件（約22億ドル相当）の輸入貨物が差し止められました³。近年はNGOやメディアによる監視強化に伴い、一次サプライヤーより先の上流まで含めた透明性確保とリスク管理を企業は求められるようになっていきます。従来、人権侵害の問題は評判上の懸念にとどまりがちでしたが、いまや訴訟など法的リスクに発展しつつあります。

気候変動に起因する異常気象や干ばつなども、企業経営にとって無視できない存在になったと言えます。2021年初頭に米国テキサス州を襲った記録的寒波では、オースティン周辺の半導体工場が停電によって操業停止に陥り、既に逼迫していた半導体サプライチェーンにさらなる打撃を与えました⁴。同年夏には中国中部・河南省での豪雨洪水によって自動車関連工場が軒並み閉鎖し、数日間にわたり生産が停まりました⁵。ESGにまつわるリスクも将来の話ではなく、既に顕在化していることが分かります。

3 <https://www.jetro.go.jp/biz/areareports/special/2023/0904/531812a91e0ffe6.html>

4 <https://www.bloomberg.com/jp/news/articles/2021-02-17/QOOV3KT1UM1101>

5 <https://www.globaltimes.cn/page/202107/1229491.shtml>

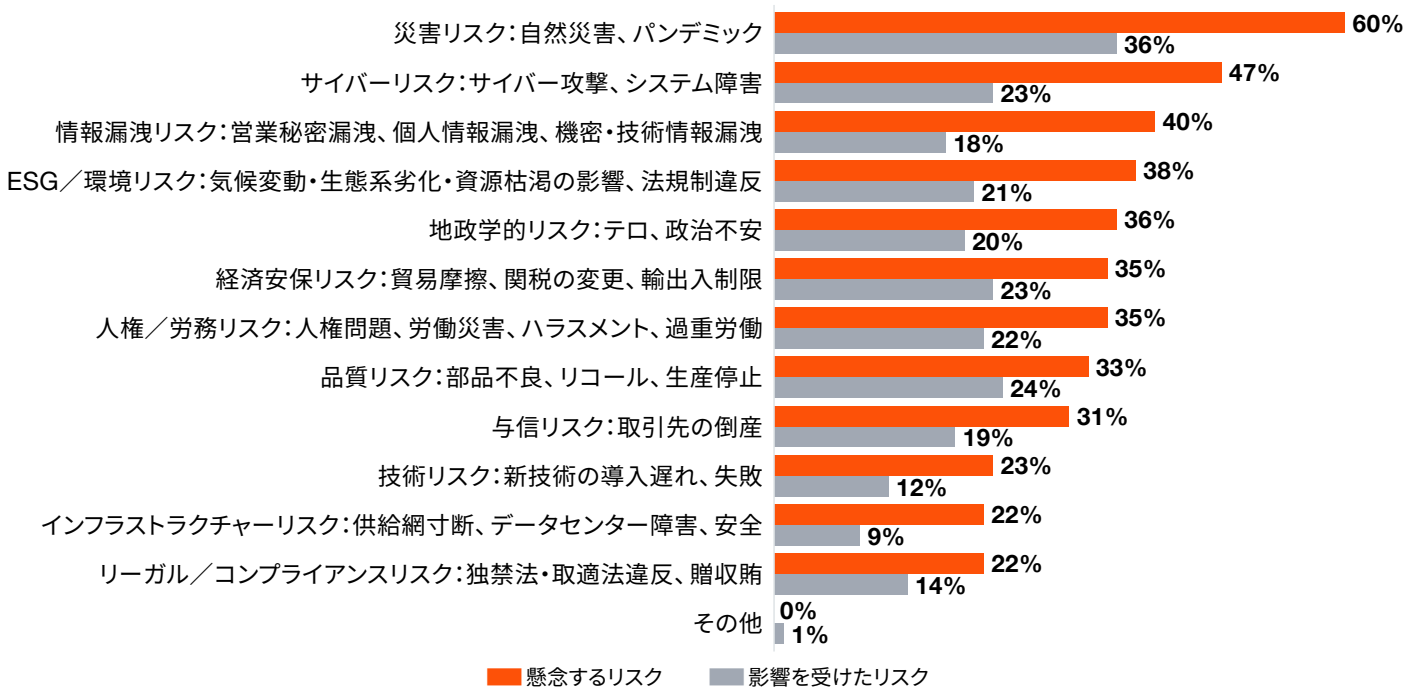


日本企業の現在地——高い認識、追いつかぬ実行

日本企業にとっても、対岸の火事ではありません。今回の調査で実際に影響を受けたサプライチェーンのリスクとしてトップとなったのが「災害」(36%)で、「ESG／環境」は21%、「人権／労務」は22%でした⁶(図表17)。

図表17：懸念するリスクと影響を受けたリスク(再掲)

Q. 貴社が懸念するサプライチェーン上のリスクおよび実際に影響を受けている／過去に影響を受けたリスクは何ですか。



出所：PwC作成

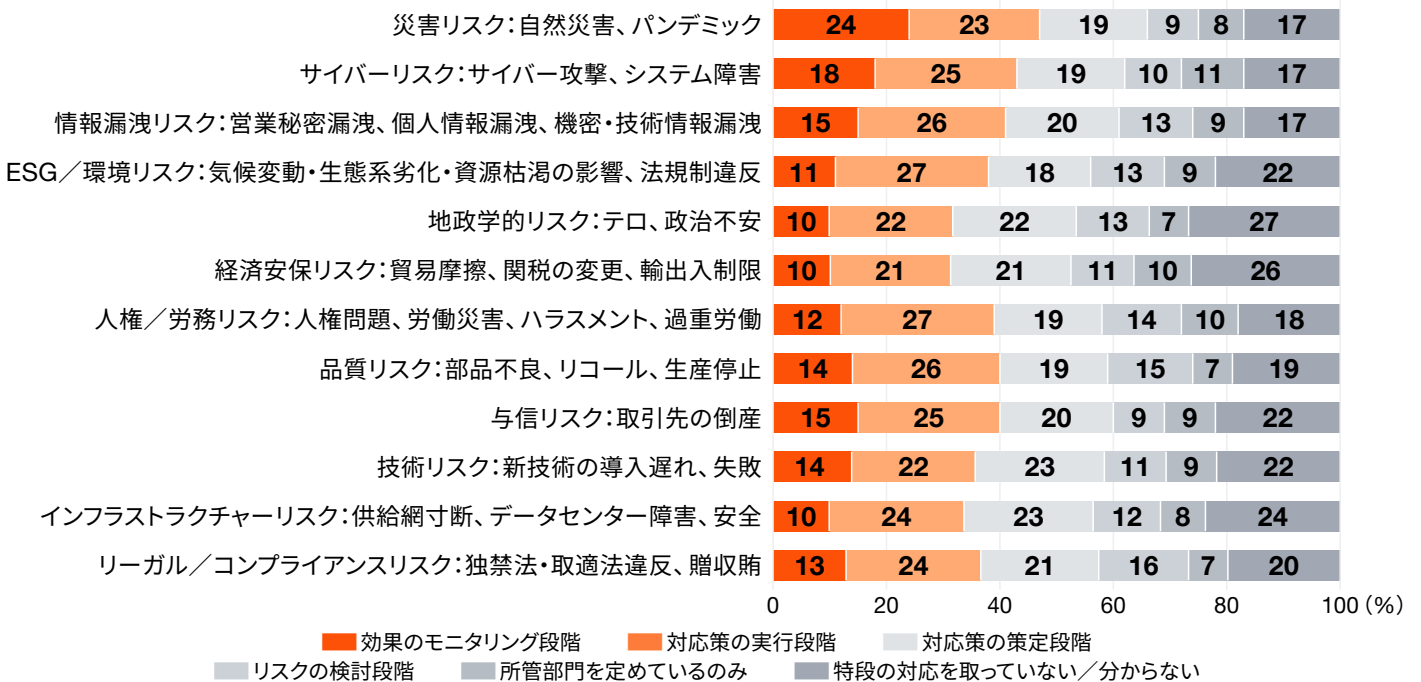
一方、調査のうち経営者にフォーカスすると、懸念するリスクは「災害」が58%、「ESG／環境」が45%、「人権／労務」が38%となっています。実際に影響を受けたリスクは「災害」と「ESG／環境」が32%、「人権／労務」が31%で、経営者の方がESGリスクに対する認識が高いことが分かります。

⁶ 本調査では、ESG／環境リスクとは気候変動・生態系劣化・資源枯渇の影響、ESG関連指令・環境規制違反などであり、災害リスクは自然災害やパンデミックを指す。近年の災害には気候変動が原因と考えられるものも多くある。なお、災害については別の項目で詳細説明する

対策は進んでいるのでしょうか。対応のフェーズを「検討(所管部門を定めているのみ、リスクの検討段階、対応策の策定段階)」と「実行(対応策の実行段階、効果のモニタリング段階)」に大別すると、最も進んでいる「災害」でさえ実行フェーズにあるのは47%と半数を下回り、「ESG/環境」は38%、「人権/労務」は39%でした。経営者の回答でも実行フェーズにある割合は「ESG/環境」が30%、「人権/労務」が26%で、高い認識を持ちつつも実行は初期的な段階にとどまっている実態が浮かびます(図表18)。

図表18：リスクへの対応状況(再掲)

Q. 貴社におけるサプライチェーンリスクへの対応状況について、それぞれ最も近いものをお選びください。



※四捨五入をしているため合計しても必ずしも100とはならない

出所：PwC作成

実務の壁をどう越えるか——リスクベースで優先順位見極めを

実行が追いつかない要因の1つが、リスク影響度の評価が財務的な算定に偏りがちな点です。売上や事業継続への影響額は見積もれても、ESG関連のレピュテーション毀損やステークホルダーへの影響といった非財務領域のリスクは、定量化が難しいために過小評価されやすい傾向にあります。

しかし本調査が示すとおり、ESG/環境や人権/労務のリスクは既に2割超の企業で実害として顕在化しています。財務的な算定だけでは捉えきれないリスクが現実のものとなっている以上、非財務の視点を評価軸に組み込み、リスクを多角的に捉え直すことが出発点となります。

その上で、実務上の壁として立ちはだかるのが、サプライチェーンの不透明性(多層にわたる取引先の実態把握の困難さ)や社内の体制不足、サプライヤー側の対応力などです。企業は自社の直接取引先にとどまらずサプライチェーン全体を可視化し、リスクを把握・管理する努力が求められます。

先進企業の中には、リスクの大小に応じて優先順位を定め(リスクベースアプローチ)、サプライヤーと協働して改善に取り組む動きも出てきました。OECD多国籍企業行動指針やCSDDD(企業持続可能性デューデリジェンス指令)などの国際基準でも、企業がバリューチェーン全域で最も深刻なリスクから順次対処していくことが求められています。まずは自社のサプライチェーンがどこに依存しているかを可視化した上で、ESGに限らず供給網全体のリスクを俯瞰し、優先度をつけて対策を検討すべきでしょう。

なお、業種によって直面するリスクの種類や優先度は異なります。本調査では、消費財・小売業界の経営陣は「ESG／環境」を最も高いリスクと考える傾向が強く、次いで「災害」、その他(「地政学」、「人権／労務」など)の順でした。一方、エネルギー・公益・鉱業業界では「地政学」を最重要視する傾向が見られ、次いで「災害」、「ESG／環境」の順となりました。

迫る規制の波 Scope3開示義務化がもたらす構造転換

では、こうしたリスクへの対応を迫る規制の動きはどうなっているのでしょうか。環境や人権関連の規制強化は揺り戻しもありますが、全体の潮流が変わったわけではなく、企業経営にとって引き続き重要なテーマです。特に激しい動きが予測されるのが、気候変動の領域でしょう。

科学的根拠に基づく温室効果ガス削減目標(SBT:Science Based Targets)の設定や、炭素税・排出量取引などカーボンプライシングの導入が世界的に進んでいます。SBTイニシアチブ(SBTi)には2026年初頭までに世界で1万社超が参加(削減目標検証済み企業数)しており、各国の炭素税・排出取引制度も2023年時点で世界排出量の約23%をカバーするに至りました。

日本でもSSBJ(サステナビリティ基準委員会)が2025年3月に気候変動関連の開示基準を公表。バリューチェーン全体を対象とした温室効果ガス(GHG)排出量(Scope3)の開示義務化も決まりました。この基準は2027年3月期より時価総額の大きい企業から順次適用される予定で、日本企業にとっても、サプライチェーンを含む自社のGHG排出の把握と削減策の実行は待ったなしです。

また、SSBJのベースとなっているISSB(国際サステナビリティ基準審議会)は2025年11月、生物多様性・自然に関する開示基準をTNFD(自然関連財務情報開示タスクフォース)に基づき策定する方針を決定。2026年10月の生物多様性条約COP17にて、「自然関連開示に関するIFRS実務記述書」の草案として公開する予定です。

2026年5月にはTISFD(不平等・社会関連財務情報開示タスクフォース)が第一草案を公開しています。2027年に最終版を取りまとめる予定ですが、TISFDのビジョンによれば、公開から2~3年で義務的／非義務的な枠組みに組み込んでいくことを目指しており、既にISSBなどのルールセッターと連携しています。生物多様性や、人権・人的資本についても、法定開示の枠組みの中で、サプライチェーン全体を対象に統合的な対応が求められてくるであろうことは想像に難くありません。

図表19：サステナビリティ関連の主な規制

名称	規制／ソフトロー	概要	動向
SSBJ (Sustainability Standards Board of Japan)	規制	日本のサステナビリティ情報開示基準の策定組織	2025年3月に気候変動関連の開示基準を公表し、バリューチェーン全体を対象とした温室効果ガス排出量 (Scope3) の開示義務化を決定
カーボンプライシング	規制	炭素税・排出量取引などの各国規制	各国・地域が導入を進める。日本は2026年よりGX-ETSと呼ばれる排出量取引の仕組みが開始
ISSB (International Sustainability Standards Board)	ソフトロー	国際会計基準を策定するIFRS財団傘下の、国際サステナビリティ基準審議会	2025年11月、「生物多様性・生態系・生態系サービス (BEES)」に関する開示基準を新たに策定することを決定 (将来的にSSBJに反映される可能性が高い)
SBT (Science Based Targets)	ソフトロー	パリ協定が求める基準と整合した、企業・団体が設定する温室効果ガス排出削減目標	2026年初頭までに世界で1万社超が参加 (削減目標検証済み企業数)
TISFD (Taskforce on Inequality and Social-related Financial Disclosures)	ソフトロー	不平等・社会関連財務情報開示タスクフォース。企業や金融機関が不平等・社会関連の情報を開示するためのグローバルなフレームワークの開発・提供を行う	2026年5月に第一草案を公開。2027年に最終版を取りまとめ、公開から2～3年で義務的／非義務的な枠組みへの組み込みを目指す。既にISSBとも連携

出所：PwC作成

環境・人権対応 サプライヤーぐるみの発想が必須に

こうした規制強化の波を受け、サプライヤーを巻き込んだ対応に踏み出す企業が日本でも増えつつあります。

取り組みが広がる領域の1つが、GHG排出量の削減。製造業や流通業ではScope3と呼ばれるサプライチェーン全体のGHG排出割合が大きく、特に調達 (Category1) や物流 (Category4・9) に関わるGHG排出量削減が喫緊の課題です。自社の省エネや再生可能エネルギー導入などと異なり、サプライヤーがGHG排出量削減成果を出して初めて自社のScope3削減が実現するため、排出実績 (1次データ) の情報提供や、削減協力の働きかけが欠かせません。

ある輸送機器メーカーは、サプライヤーと自社の間で共有可能なデータプラットフォーム上に、排出量の入力・算定を可能とする独自モデルを開発・実装しました。Scope3のGHG排出の可視化から削減施策の策定、サプライヤーとのコミュニケーションまでを一貫して行える体制を構築し、GHG排出量削減を実現しています。これら一連の活動、すなわちサプライヤーエンゲージメントにおいては、業務フローの改革やサプライヤー対応の教育も不可欠です。同社では標準業務フローの整備・構築に加え、それを運用する専門人材の育成にも力を注いでいます。

また、あるエンターテインメント業界の大手では、OECD多国籍企業行動指針や欧州のCSDDD、TNFDなど国際的な枠組みを参照し、同一のサプライヤー情報を基に人権・環境の双方からリスク評価を実施しました。全てのサプライヤーを初期から網羅することは困難なため、取引規模や調達品目の重要度、サプライヤー企業の業態・規模に応じて優先度を設定し、重要度の高い先から段階的に評価するリスクベースのアプローチを採用しています。

人権面の評価では、自社情報に加え、業界で顕在化しやすいリスクを把握するために、競合他社の事例も収集。自社で同様のリスクが生じる可能性について関係者にヒアリングするなど、内外の情報を統合してリスクの特定と評価をしました。

環境面の評価では、膨大な数のサプライヤーをリスクの多寡に応じて絞り込むため、事業内容(自然環境への悪影響の可能性)と所在地(被害が深刻化し得る地域か)の2軸で、優先度を判定しています。これにより高リスクの可能性がある先を特定でき、今後の個社デューデリジェンスに向けたステップに踏み出す準備が整いました。

ESGデューデリジェンスは「受け身のコスト」にあらず

環境・人権のデューデリジェンスの実践は、不確実性の増す世界で事業のレジリエンスを高めるために必要不可欠な戦略的投資です。

検討すべきリスクの質や優先度は業種によって異なりますが、まずは自社の供給網がどのような自然資本・人的資本に依存し、それらにどのような影響を与えているかを可視化した上で、サプライチェーン全体のリスクに優先順位をつけて対策を講じるべきです。

ただ、本調査が示したとおり、ESG／環境や人権／労務のリスクを認識しながらも、実行フェーズには3割前後しか達していません。リスクを認識しつつ対策に踏み出せない構図は、サプライチェーンリスク管理全般に共通しますが、とりわけESG領域では、対応を規制への「受け身のコスト」と捉える意識が、この傾向に拍車をかけているのではないのでしょうか。

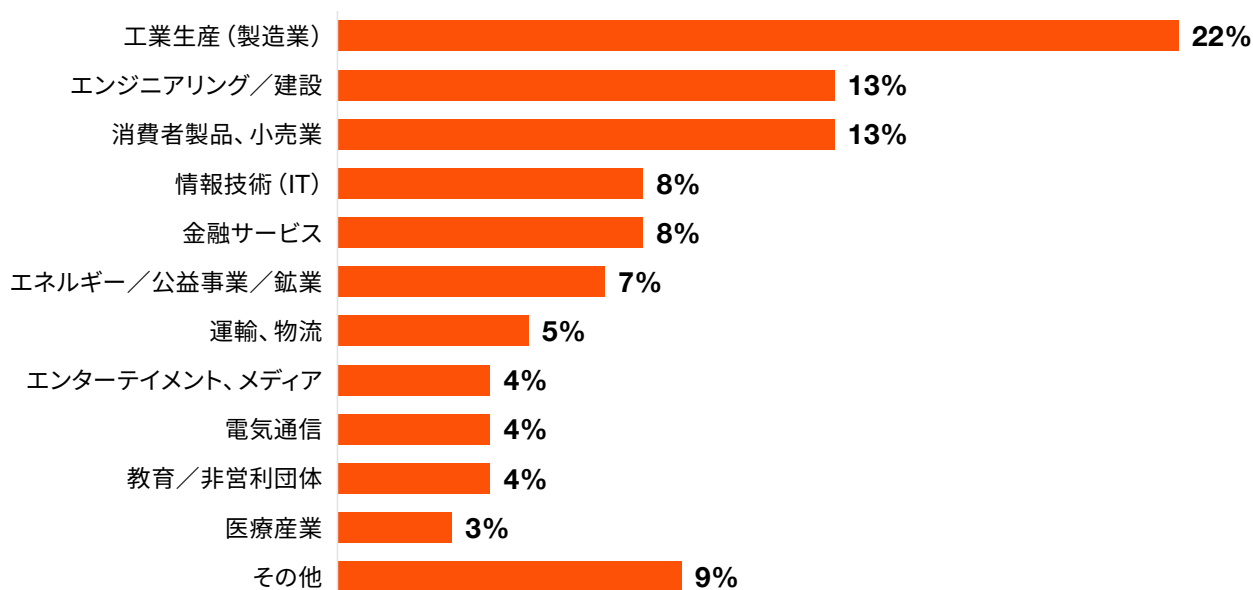
サプライチェーン上の環境負荷や人権侵害は本来、複雑な供給網の中に埋もれ、ある日突然、規制違反・訴訟・取引停止・レピュテーション毀損といった形で顕在化します。デューデリジェンスとは、こうした「見えないコスト」を先回りして可視化し、管理可能な状態に変える営みです。

さらに言えば、サプライヤーとの協働でGHG排出量削減や人権課題に取り組むプロセスは、供給網全体の透明性を高める他、取引先との信頼関係を深め、そのレジリエンスを強化します。ESGデューデリジェンスは、サプライチェーン全体の競争力を高める起点となりうるのです。

ESGデューデリジェンスを「受け身のコスト」にとどめるのか、「戦略的投資」と捉えるのか。その判断を日本企業は迫られています。

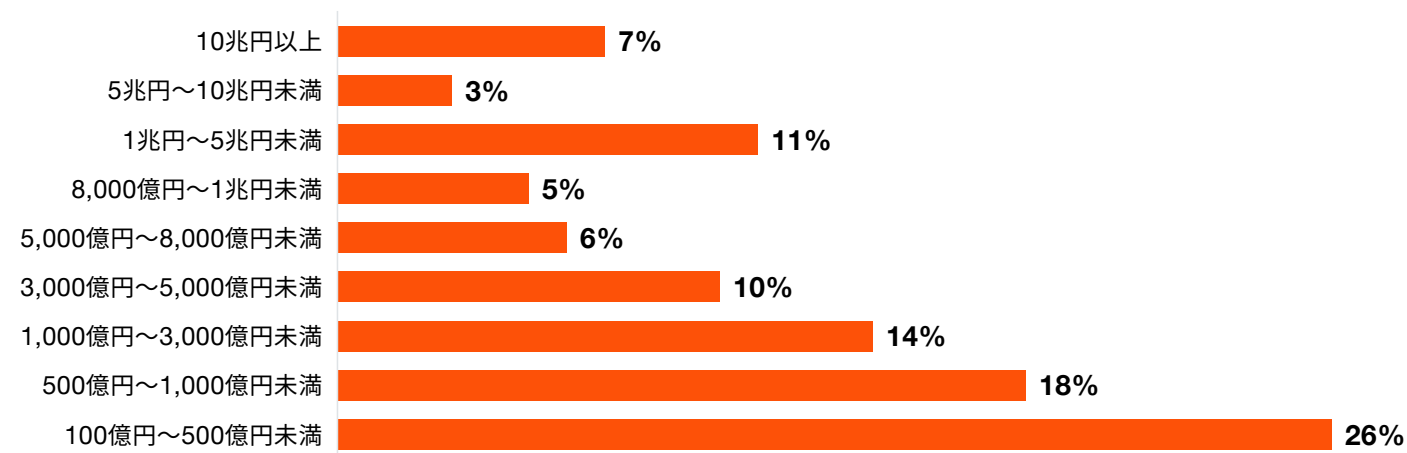
参考データ

図表20：回答者属性情報(業種)



出所：PwC作成

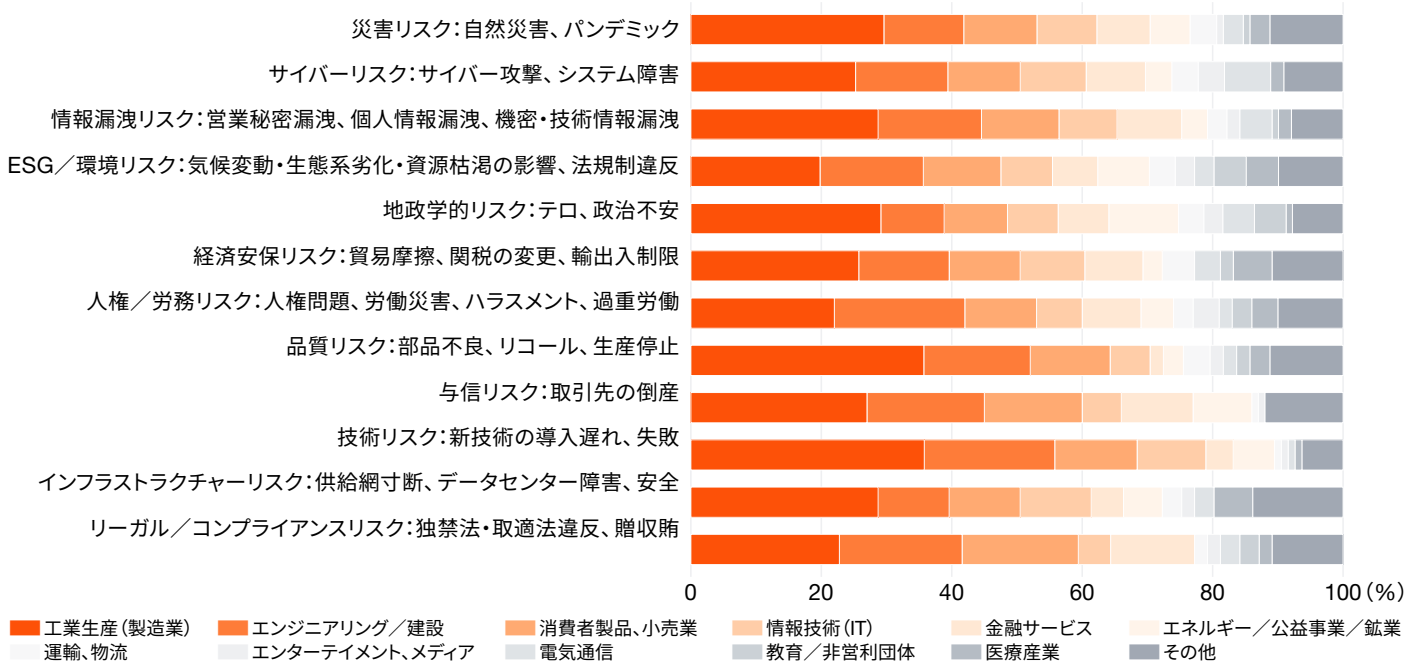
図表21：回答者属性情報(売上高)



出所：PwC作成

図表22：懸念するリスク(業種別)

Q. 貴社が懸念するサプライチェーン上のリスクは何ですか。

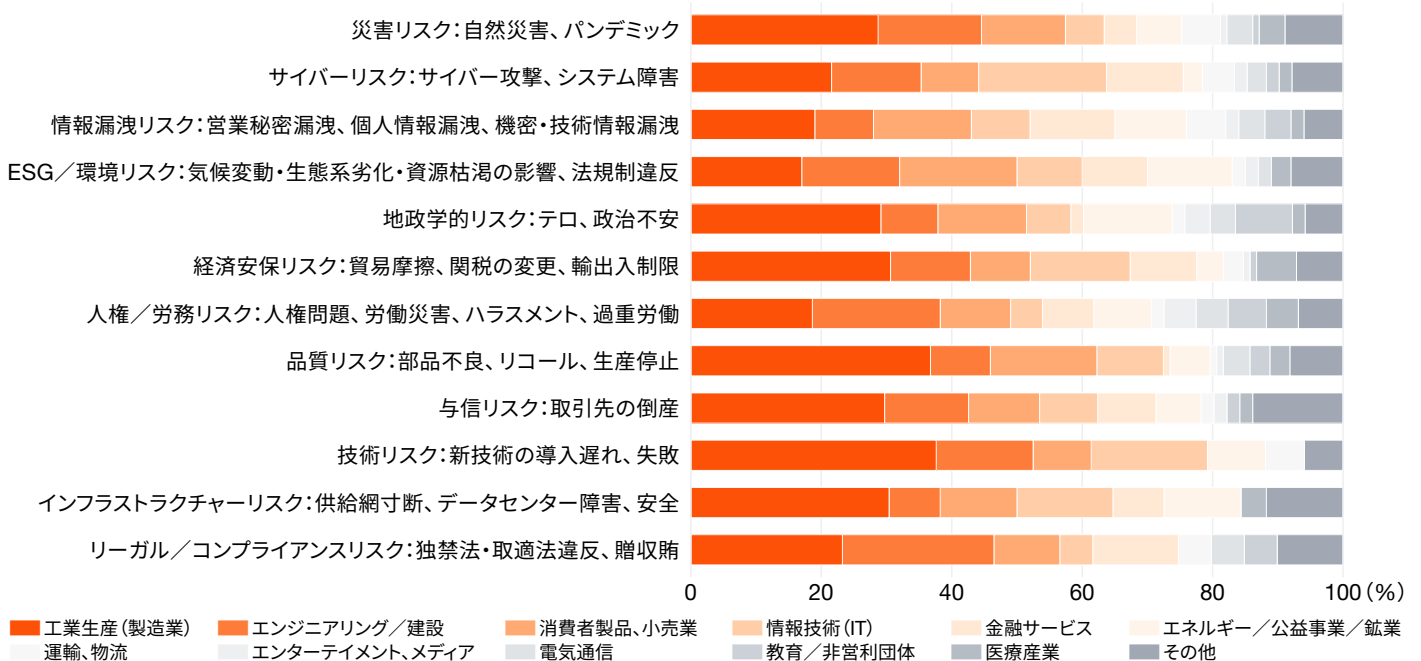


※四捨五入をしているため合計しても必ずしも100とはならない

出所：PwC作成

図表23：影響を受けたリスク(業種別)

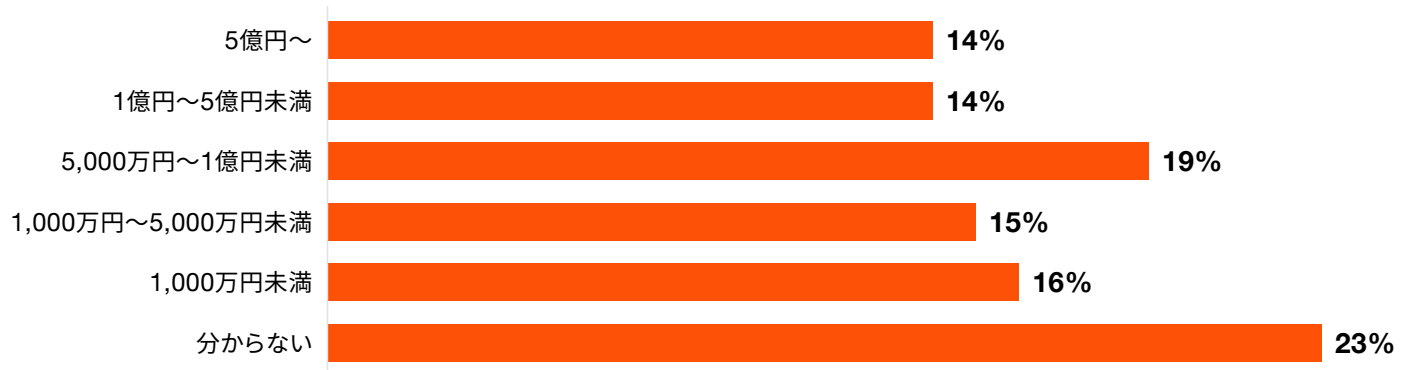
Q. 貴社が実際に影響を受けている/過去に影響を受けたリスクは何ですか。



※四捨五入をしているため合計しても必ずしも100とはならない

出所：PwC作成

図表24：サプライチェーンリスクの管理に対する現在の投資額



出所：PwC作成





PwC Japanグループ

<https://www.pwc.com/jp/ja/contact.html>



www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社 (PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む) の総称です。各法人は独立した別法人として事業を行っています。

複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約13,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。

PwCは、クライアントが複雑性を競争優位性へと転換できるよう、信頼の構築と変革を支援します。私たちは、テクノロジーを駆使し、人材を重視したネットワークとして、世界137の国と地域に364,000人以上のスタッフを擁しています。監査・保証、税務・法務、アドバイザリーサービスなど、多岐にわたる分野で、クライアントが変革の推進力を生み出し、加速し、維持できるよう支援します。

発行年月：2026年6月

管理番号：I202602-06

© 2026 PwC. All rights reserved.

PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.